	Type	Hits	Search Text
1	IS&R	1053	((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.
2	BRS	240	(((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.) and (portable or pager or cell$phone or mobile$phone or pda)
3	BRS	67	((((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.) and (portable or pager or cell$phone or mobile$phone or pda)) and (radio)
4	BRS	63	(((((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.) and (portable or pager or cell$phone or mobile$phone or pda)) and (radio)) and (frequency or signal)
5	BRS	55	((((((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.) and (portable or pager or cell$phone or mobile$phone or pda)) and (radio)) and (frequency or signal)) and digital
6	BRS	24	(((((((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.) and (portable or pager or cell$phone or mobile$phone or pda)) and (radio)) and (frequency or signal)) and digital) and (balance and store)
7	BRS	24	(((((((((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.) and (portable or pager or cell$phone or mobile$phone or pda)) and (radio)) and (frequency or signal)) and digital) and (balance and store)) and card
8	BRS	12	((((((((((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.) and (portable or pager or cell$phone or mobile$phone or pda)) and (radio)) and (frequency or signal)) and digital) and (balance and store)) and card) and (electronic near (money or funds))
9	BRS	145215	portable or pager or cell$phone or mobile$phone or pda
10	BRS	28144	(portable or pager or cell$phone or mobile$phone or pda) and radio
11	BRS	25102	((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)

	Type	Hits	Search Text
12	BRS	15096	(((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital
13	BRS	1073	((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store and balance)
14	BRS	654	(((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store and balance)) and card
15	BRS	92	((((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store and balance)) and card) and (electronic near (funds or cash or money))
16	BRS	92	(((((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store and balance)) and card) and (electronic near (funds or cash or money))) and card
17	BRS	3	((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store near balance)
18	BRS	92	(((((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store and balance)) and card) and (electronic near (funds or cash or money))) and card) not (((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store near balance))

	Type	Hits	Search Text
19	BRS	77	((((((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store and balance)) and card) and (electronic near (funds or cash or money))) and card) not (((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store near balance))) not ((((((((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.) and (portable or pager or cell$phone or mobile$phone or pda)) and (radio)) and (frequency or signal)) and digital) and (balance and store)) and card)
20	BRS	6	(((((((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store and balance)) and card) and (electronic near (funds or cash or money))) and card) not (((((portable or pager or cell$phone or mobile$phone or pda) and radio) and (frequency or signal)) and digital) and (store near balance))) not ((((((((705/35) or (705/39) or (705/41) or (705/42) or (705/44)).CCLS.) and (portable or pager or cell$phone or mobile$phone or pda)) and (radio)) and (frequency or signal)) and digital) and (balance and store)) and card)) and ((portable or wireless).ab.ti.)
21	BRS	1	"6032858".PN.
22	BRS	1	"5962833".PN.
23	BRS	1	"5857152".PN.
24	BRS	1	"5806045".PN.
25	BRS	1	"5751973".PN.
26	BRS	1	"5714741".PN.
27	BRS	1	"5698837".PN.
28	BRS	1	"5698837".PN.

	Type	Hits	Search Text
29	BRS	1	"5691525".PN.
30	BRS	1	"5933816".PN.
31	BRS	1	"5748737".PN.
32	BRS	1	"5721781".PN.
33	BRS	1	"5701414".PN.
34	BRS	1	(US-6311167-$).did.
35	BRS	0	((US-6311167-$).did.) and (format same (error or valid or correct))
36	BRS	1	((US-6311167-$).did.) and (error)
37	BRS	1	(((US-6311167-$).did.) and (error)) and (radio same digital)
38	BRS	8	(US-6539362-$ or US-6311167-$ or US-5930363-$ or US-6536661-$ or US-6466783-$ or US-6032858-$ or US-5714741-$ or US-5748737-$).did.
39	BRS	8	((US-6539362-$ or US-6311167-$ or US-5930363-$ or US-6536661-$ or US-6466783-$ or US-6032858-$ or US-5714741-$ or US-5748737-$).did.) and (judging or compar$3 or certification or verify$3)
40	BRS	8	(((US-6539362-$ or US-6311167-$ or US-5930363-$ or US-6536661-$ or US-6466783-$ or US-6032858-$ or US-5714741-$ or US-5748737-$).did.) and (judging or compar$3 or certification or verify$3)) and ((account or balance or personal) same (information or data))
41	BRS	6	((((US-6539362-$ or US-6311167-$ or US-5930363-$ or US-6536661-$ or US-6466783-$ or US-6032858-$ or US-5714741-$ or US-5748737-$).did.) and (judging or compar$3 or certification or verify$3)) and ((account or balance or personal) same (information or data))) and radio
42	BRS	8	(US-6539362-$ or US-6311167-$ or US-5930363-$ or US-6536661-$ or US-6466783-$ or US-6032858-$ or US-5714741-$ or US-5748737-$).did.

	Type	Hits	Search Text
43	BRS	6	((US-6539362-$ or US-6311167-$ or US-5930363-$ or US-6536661-$ or US-6466783-$ or US-6032858-$ or US-5714741-$ or US-5748737-$).did.) and (compare and number)
44	BRS	4	(((US-6539362-$ or US-6311167-$ or US-5930363-$ or US-6536661-$ or US-6466783-$ or US-6032858-$ or US-5714741-$ or US-5748737-$).did.) and (compare and number)) and radio
45	BRS	1812	radio and number and compare and card and store and account
46	BRS	655	(radio and number and compare and card and store and account) and balance
47	BRS	446	((radio and number and compare and card and store and account) and balance) and ((compare or authenticate or verify) same (number or code))
48	BRS	128	(((radio and number and compare and card and store and account) and balance) and ((compare or authenticate or verify) same (number or code))) and ((radio or rf) near (signal))
49	BRS	128	((((radio and number and compare and card and store and account) and balance) and ((compare or authenticate or verify) same (number or code))) and ((radio or rf) near (signal))) and (data and information)
50	BRS	54	(replenish or refill or reload) near card
51	BRS	10	((replenish or refill or reload) near card) and (radio or rf)
52	BRS	272	MSISDN
53	BRS	110	MSISDN and card
54	BRS	70	(replenish or refill or reload refresh) near card
55	BRS	1576	(replenish or refill or reload refresh) same (card or account)
56	BRS	299	((replenish or refill or reload refresh) same (card or account)) and (radio or rf)
57	IS&R	1536	(705/35-42).CCLS.

	Type	Hits	Search Text
58	BRS	13	(((replenish or refill or reload refresh) same (card or account)) and (radio or rf)) and ((705/35-42).CCLS.)
59	BRS	12	((((replenish or refill or reload refresh) same (card or account)) and (radio or rf)) and ((705/35-42).CCLS.)) and ((compare or authenticate or verify) same (number or code))
60	BRS	12	(((((replenish or refill or reload refresh) same (card or account)) and (radio or rf)) and ((705/35-42).CCLS.)) and ((compare or authenticate or verify) same (number or code))) and (data and information)
61	BRS	9	((((((replenish or refill or reload refresh) same (card or account)) and (radio or rf)) and ((705/35-42).CCLS.)) and ((compare or authenticate or verify) same (number or code))) and (data and information)) and (radio and number and compare and card and store and account)
62	BRS	8864	(stored or pre$paid or smart) near card
63	BRS	5950	((stored or pre$paid or smart) near card) and store
64	BRS	1666	(((stored or pre$paid or smart) near card) and store) and radio
65	BRS	1076	((((stored or pre$paid or smart) near card) and store) and radio) and (compar$3)
66	BRS	1065	(((((stored or pre$paid or smart) near card) and store) and radio) and (compar$3)) and (number or pin)
67	BRS	323	((((((stored or pre$paid or smart) near card) and store) and radio) and (compar$3)) and (number or pin)) and balance
68	BRS	202	(((((((stored or pre$paid or smart) near card) and store) and radio) and (compar$3)) and (number or pin)) and balance) and ((personal or user or customer or subscriber) near (information or data or profile))

	Type	Hits	Search Text
69	BRS	64	(((((((stored or pre$paid or smart) near card) and store) and radio) and (compar$3)) and (number or pin)) and balance) and ((personal or user or customer or subscriber) near (information or data or profile))) and ((compr$3) same (number or pin))
70	IS&R	198	(705/41).CCLS.
71	BRS	2	((((((((stored or pre$paid or smart) near card) and store) and radio) and (compar$3)) and (number or pin)) and balance) and ((personal or user or customer or subscriber) near (information or data or profile))) and ((compr$3) same (number or pin))) and ((705/41).CCLS.)
72	IS&R	360	(705/39).CCLS.
73	BRS	2	((((((((stored or pre$paid or smart) near card) and store) and radio) and (compar$3)) and (number or pin)) and balance) and ((personal or user or customer or subscriber) near (information or data or profile))) and ((compr$3) same (number or pin))) and ((705/39).CCLS.)
74	BRS	5741	(((stored or pre$paid or smart) near card) and store) and (number or pin)
75	BRS	1402	((((stored or pre$paid or smart) near card) and store) and (number or pin)) and balance
76	BRS	345	(((((stored or pre$paid or smart) near card) and store) and (number or pin)) and balance) and ((compr$3) same (number or pin))
77	IS&R	675	(705/39-41).CCLS.
78	BRS	32	((((((stored or pre$paid or smart) near card) and store) and (number or pin)) and balance) and ((compr$3) same (number or pin))) and ((705/39-41).CCLS.)
79	BRS	8	(((((((stored or pre$paid or smart) near card) and store) and (number or pin)) and balance) and ((compr$3) same (number or pin))) and ((705/39-41).CCLS.)) and (radio or rf)

	Type	Hits	Search Text
80	IS&R	1	("6726098").PN.
81	BRS	1	(US-6536661-$).did.
82	BRS	0	((US-6536661-$).did.) and (store near balance)
83	BRS	1	"6032858".PN.
84	BRS	1	"5962833".PN.
85	BRS	1	"5857152".PN.
86	BRS	1	"5806045".PN.
87	BRS	1	"5714741".PN.
88	BRS	273	msisdn
89	BRS	3	msidn
90	BRS	0	((705/39-41).CCLS.) and (msisdn and number)
91	BRS	271	msisdn and number
92	BRS	10	(US-6311167-$ or US-6539362-$ or US-6105006-$ or US-5930363-$ or US-6536661-$ or US-6466783-$ or US-6032858-$ or US-5714741-$ or US-5748737-$ or US-6726098-$).did.
93	BRS	3	((US-6311167-$ or US-6539362-$ or US-6105006-$ or US-5930363-$ or US-6536661-$ or US-6466783-$ or US-6032858-$ or US-5714741-$ or US-5748737-$ or US-6726098-$).did.) and error

US006105006A

United States Patent [19]

Davis et al.

[11] Patent Number: 6,105,006

[45] Date of Patent: Aug. 15, 2000

[54] **TRANSACTION AUTHENTICATION FOR 1-WAY WIRELESS FINANCIAL MESSAGING UNITS**

[76] Inventors: **Walter Lee Davis**, 5820 NW. 96 Dr., Parkland, Fla. 33076; **Gregg Edward Rasor**, 1164 SW. 23rd Ave., Boynton Beach, Fla. 33426; **Philip Paul Macnak**, 14909 Horseshoe Trace, Wellington, Fla. 33414

[21] Appl. No.: **08/996,179**

[22] Filed: **Dec. 22, 1997**

[51] **Int. Cl.**[7] **G07F 7/08**; H04L 9/00

[52] **U.S. Cl.** **705/35**; 705/35; 705/39; 705/40; 705/41; 705/42; 380/4; 380/21; 380/24; 380/25; 235/379; 235/380; 357/17; 358/88

[58] **Field of Search** 705/35, 39, 40, 705/41, 42; 380/24, 4, 25; 357/17; 358/88; 310/323; 340/825; 235/379, 380

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,305,059	12/1981	Benton .	
4,424,529	1/1984	Roese et al.	358/88
4,529,870	7/1985	Chaum .	
4,575,621	3/1986	Dreifus .	
4,686,407	8/1987	Ceperley	310/323
4,707,592	11/1987	Ware .	
4,819,039	4/1989	Chi et al.	357/17
4,965,568	10/1990	Atalla et al.	340/825
5,159,632	10/1992	Crandall .	
5,192,947	3/1993	Neustein .	
5,265,033	11/1993	Vajk et al. .	
5,285,496	2/1994	Frank et al. .	
5,347,580	9/1994	Molva et al. .	
5,359,182	10/1994	Schilling .	
5,371,493	12/1994	Sharpe et al. .	

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

0172670	7/1985	European Pat. Off. .
0738992A1	10/1996	European Pat. Off. .
WO93/07596	4/1993	WIPO .
WO96/32700	3/1996	WIPO .
WO96/25828	8/1996	WIPO .
WO96/36025	11/1996	WIPO .

OTHER PUBLICATIONS

"Secure Electronic Transaction (SET) Specification", Book 1: Business Description, Draft for testing Jun. 17, 1996.

"Secure Electronic Transaction (SET) Specification," Book 2: Programmer's Guide, Draft for testing Jun. 21, 1996.

"Secure Electronic Transaction (SET) Specification", Book 3: Formal Protocol Definition, Draft for Testing Jun. 24, 1996 with revisions on Aug. 1, 1996.

"Standard for RSA, Diffie–Hellman & Related Public–Key Cryptography", Part 6: Elliptic Curve Systems (Draft 5), Working Draft.

"Electronic Documents & Digital Signaturing: Changing the Way Business is Conducted and Contracts are Formed", by Paul R. Katz & Aron Schwartz, IPL Newsletter, vol. 14, Number 2, Winter 1996.

"In Introduction to Electronic Money Issues".

"An Introduction to Electronic Money Issues" prepared for the US Dept of the Treasury Conference, Toward Electronic Money & Banking: the Role of Govt, Sep. 19–20, 1996 Washington, DC.

"Electronic Banking Law and Commerce Report", Devoted to the Emerging Law of Cyberbanking pp. 8–12–17.

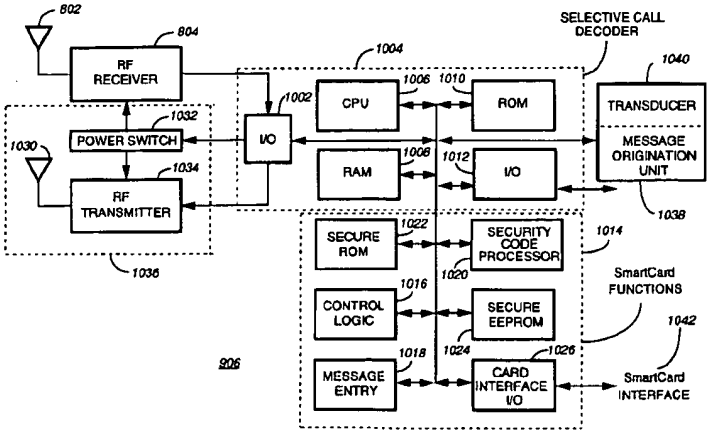
"A Standard Code for Radiopaging", British Post Officee.

Primary Examiner—James P. Trammell
Assistant Examiner—Nga B. Nguyen
Attorney, Agent, or Firm—Gregg Rasor

[57] **ABSTRACT**

A secure financial messaging unit (**906**) includes a wide area radio frequency receiver (**804**), a selective call decoder (**1004**), a financial transaction processor (**1014**), a main processor (**1006**), and a message origination unit (**1034**). The message origination unit (**1034**) operates in at least one of a reply and confirmation mode and a originate and request mode to effect a wireless financial transaction using a local area link (**924**).

39 Claims, 11 Drawing Sheets



U.S. PATENT DOCUMENTS

5,412,192	5/1995	Hoss .	
5,440,634	8/1995	Jones et al. .	
5,442,707	8/1995	Miyaji et al. .	
5,452,356	9/1995	Albert .	
5,453,601	9/1995	Rosen .	
5,455,864	10/1995	Park .	
5,467,398	11/1995	Pierce et al. .	
5,473,143	12/1995	Vak et al. .	
5,473,667	12/1995	Neustein .	
5,477,215	12/1995	Mandelbaum .	
5,481,255	1/1996	Albert et al. .	
5,483,595	1/1996	Owen .	
5,510,778	4/1996	Krieter et al. .	
5,521,363	5/1996	Tannenbaum .	
5,539,189	7/1996	Wilson .	
5,541,583	7/1996	Mandelbaum .	
5,557,518	9/1996	Rosen .	
5,572,004	11/1996	Raimann .	
5,585,787	12/1996	Wallerstein .	
5,585,789	12/1996	Haneda .	
5,590,038	12/1996	Pitroda .	
5,591,949	1/1997	Bernstein .	
5,754,655	5/1998	Hughes et al.	380/24

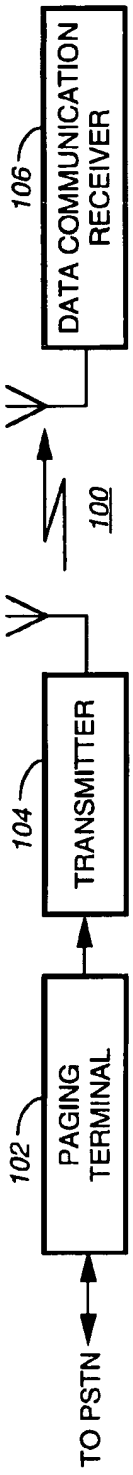

TO PSTN
102
PAGING TERMINAL
104
TRANSMITTER
100
106
DATA COMMUNICATION RECEIVER

FIG. 1

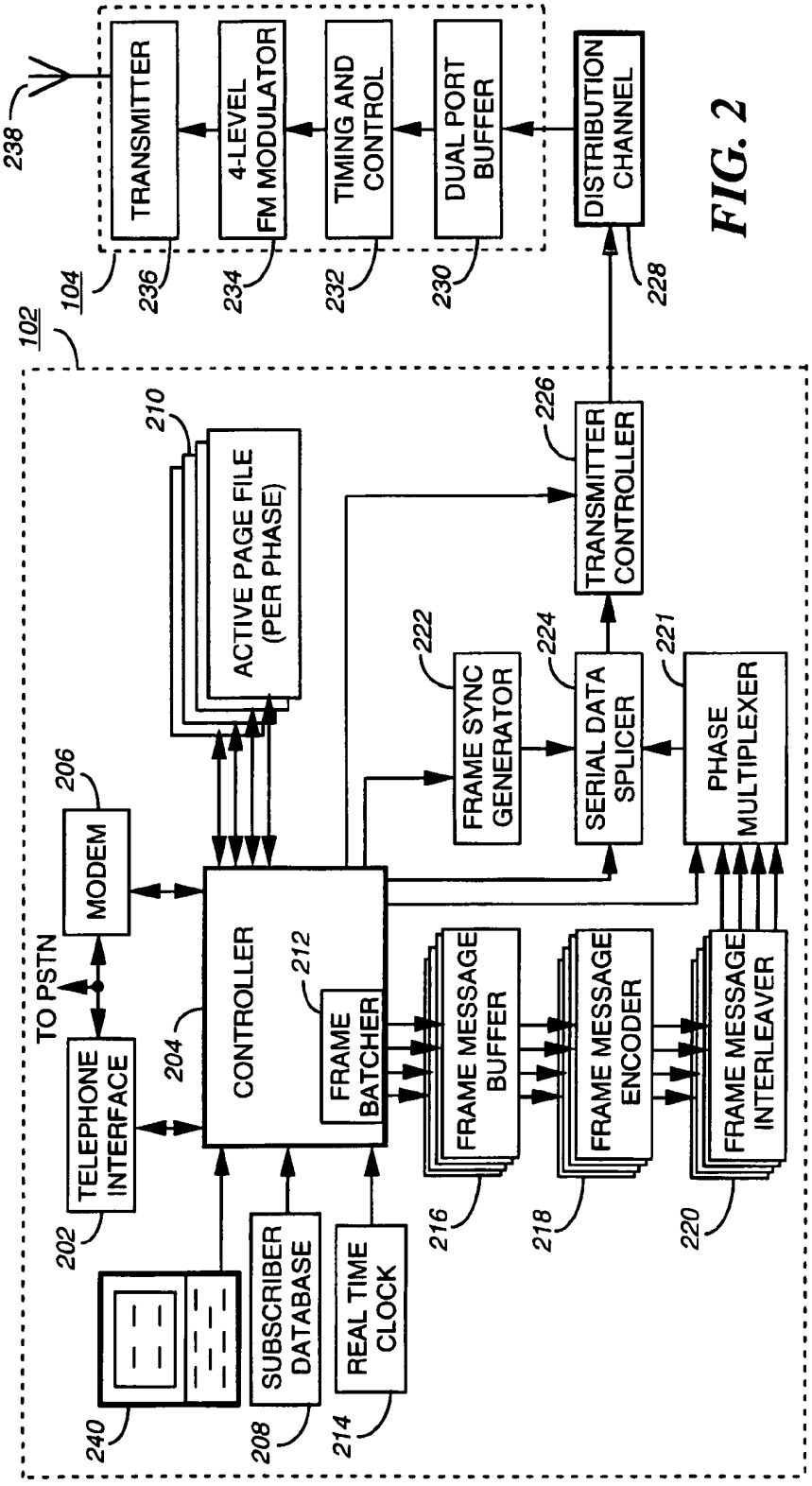

238
TRANSMITTER
4-LEVEL FM MODULATOR
TIMING AND CONTROL
DUAL PORT BUFFER
DISTRIBUTION CHANNEL
104
236
234
232
230
228
102
210
ACTIVE PAGE FILE (PER PHASE)
226
TRANSMITTER CONTROLLER
222
FRAME SYNC GENERATOR
224
SERIAL DATA SPLICER
221
PHASE MULTIPLEXER
206
MODEM
TO PSTN
TELEPHONE INTERFACE
202
204
CONTROLLER
212
FRAME BATCHER
FRAME MESSAGE BUFFER
FRAME MESSAGE ENCODER
FRAME MESSAGE INTERLEAVER
216
218
220
240
SUBSCRIBER DATABASE
208
REAL TIME CLOCK
214

FIG. 2

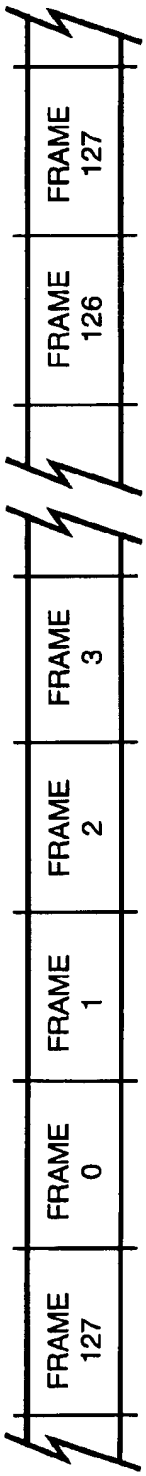


FIG. 3

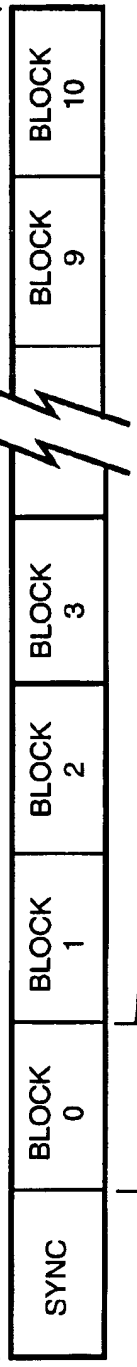


FIG. 4

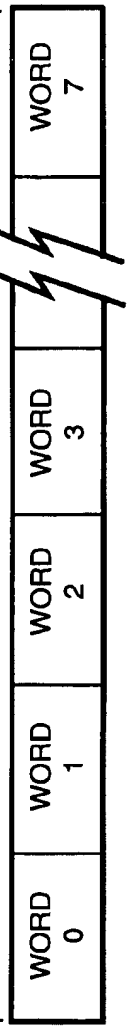


FIG. 5

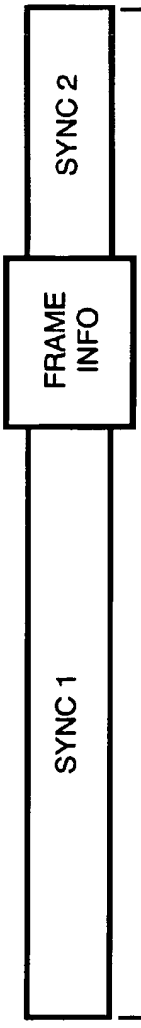


FIG. 6

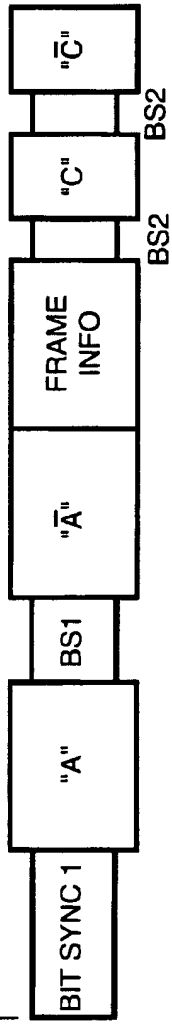
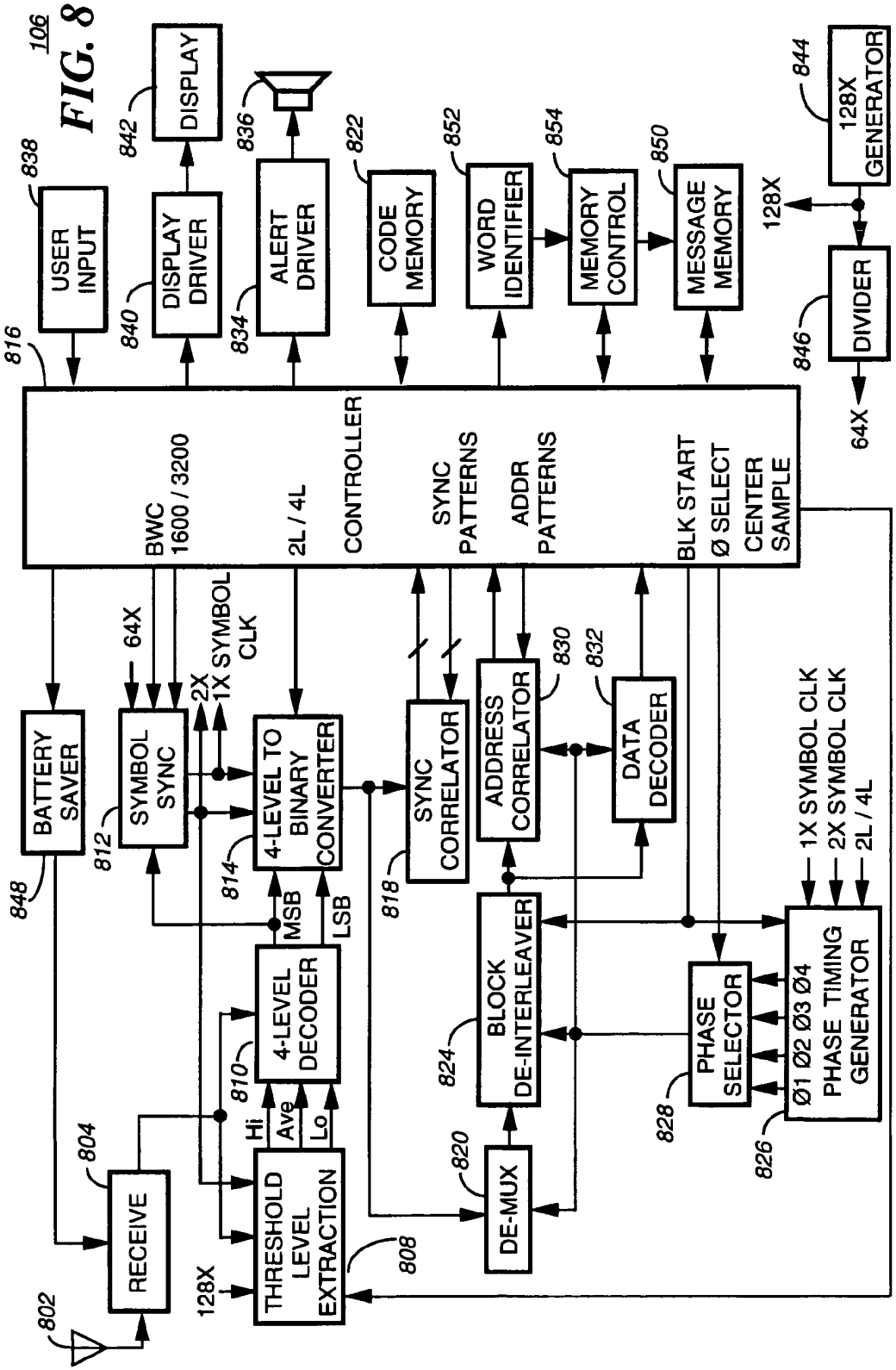


FIG. 7

FIG. 8


106
802
804
806
808
810
812
814
816
818
820
822
824
826
828
830
832
834
836
838
840
842
844
846
848
850
852
854
RECEIVE
THRESHOLD LEVEL EXTRACTION
4-LEVEL DECODER
SYMBOL SYNC
4-LEVEL TO BINARY CONVERTER
CONTROLLER
SYNC CORRELATOR
ADDRESS CORRELATOR
DATA DECODER
DE-MUX
BLOCK DE-INTERLEAVER
PHASE SELECTOR
PHASE TIMING GENERATOR
BATTERY SAVER
USER INPUT
DISPLAY DRIVER
DISPLAY
ALERT DRIVER
CODE MEMORY
WORD IDENTIFIER
MEMORY CONTROL
MESSAGE MEMORY
128X GENERATOR
DIVIDER
128X
64X
2X
1X SYMBOL CLK
MSB
LSB
Hi
Ave
Lo
BWC 1600 / 3200
2L / 4L
SYNC PATTERNS
ADDR PATTERNS
BLK START
Ø SELECT
CENTER SAMPLE
Ø1 Ø2 Ø3 Ø4
2L / 4L

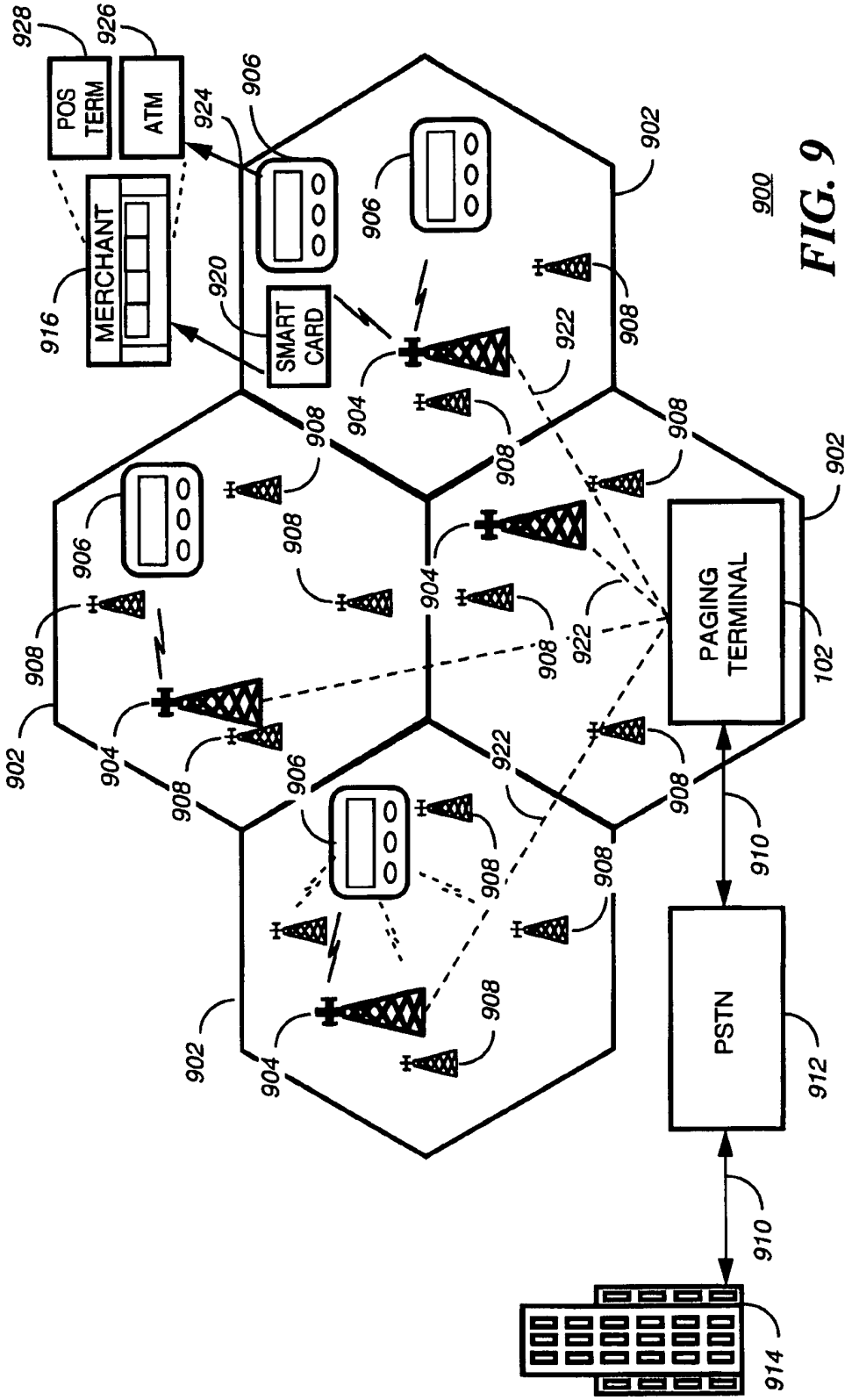

928
926
POS TERM
ATM
924
906
902
MERCHANT
916
920
SMART CARD
922
908
904
PAGING TERMINAL
102
910
PSTN
912
914
900

FIG. 9

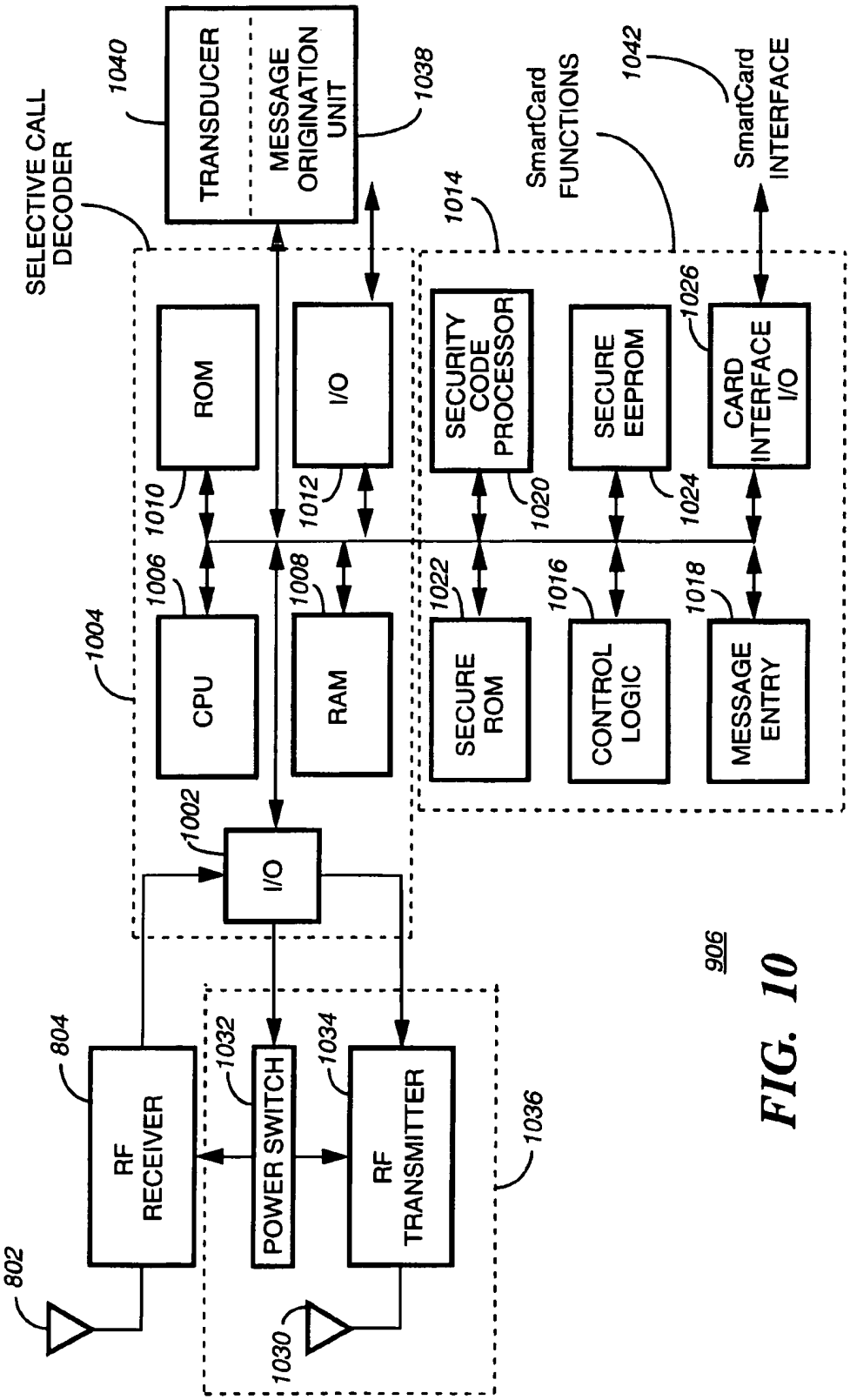

SELECTIVE CALL DECODER
1040
TRANSDUCER
MESSAGE ORIGINATION UNIT
1038
1042
SmartCard FUNCTIONS
SmartCard INTERFACE
1014
ROM
I/O
SECURITY CODE PROCESSOR
SECURE EEPROM
CARD INTERFACE I/O
1026
1010
1012
1020
1024
1006
1008
1022
1016
1018
1004
CPU
RAM
SECURE ROM
CONTROL LOGIC
MESSAGE ENTRY
1002
I/O
906
804
1032
1034
RF RECEIVER
POWER SWITCH
RF TRANSMITTER
1036
802
1030

FIG. 10

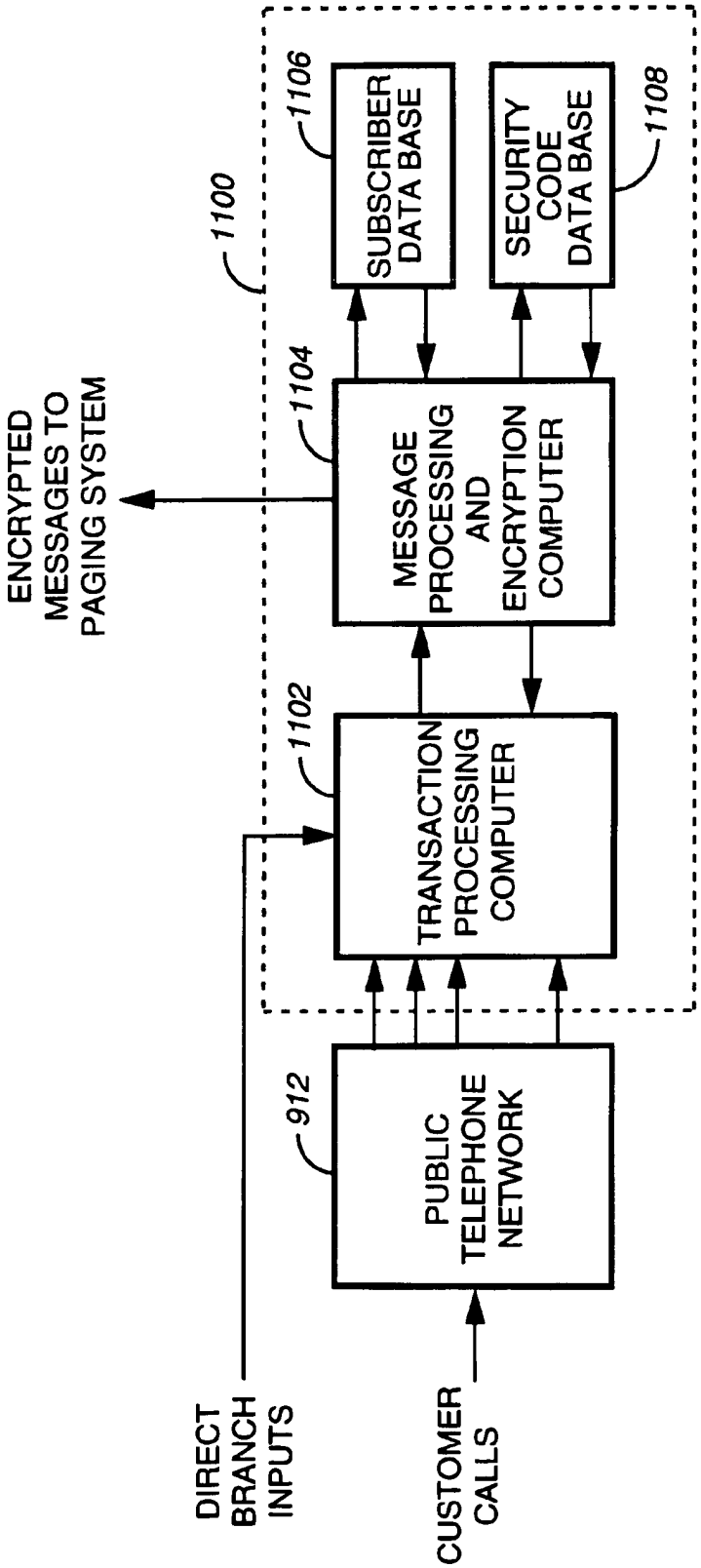

1100
1106
SUBSCRIBER DATA BASE
1108
SECURITY CODE DATA BASE
1104
MESSAGE PROCESSING AND ENCRYPTION COMPUTER
ENCRYPTED MESSAGES TO PAGING SYSTEM
1102
TRANSACTION PROCESSING COMPUTER
912
PUBLIC TELEPHONE NETWORK
DIRECT BRANCH INPUTS
CUSTOMER CALLS

FIG. 11

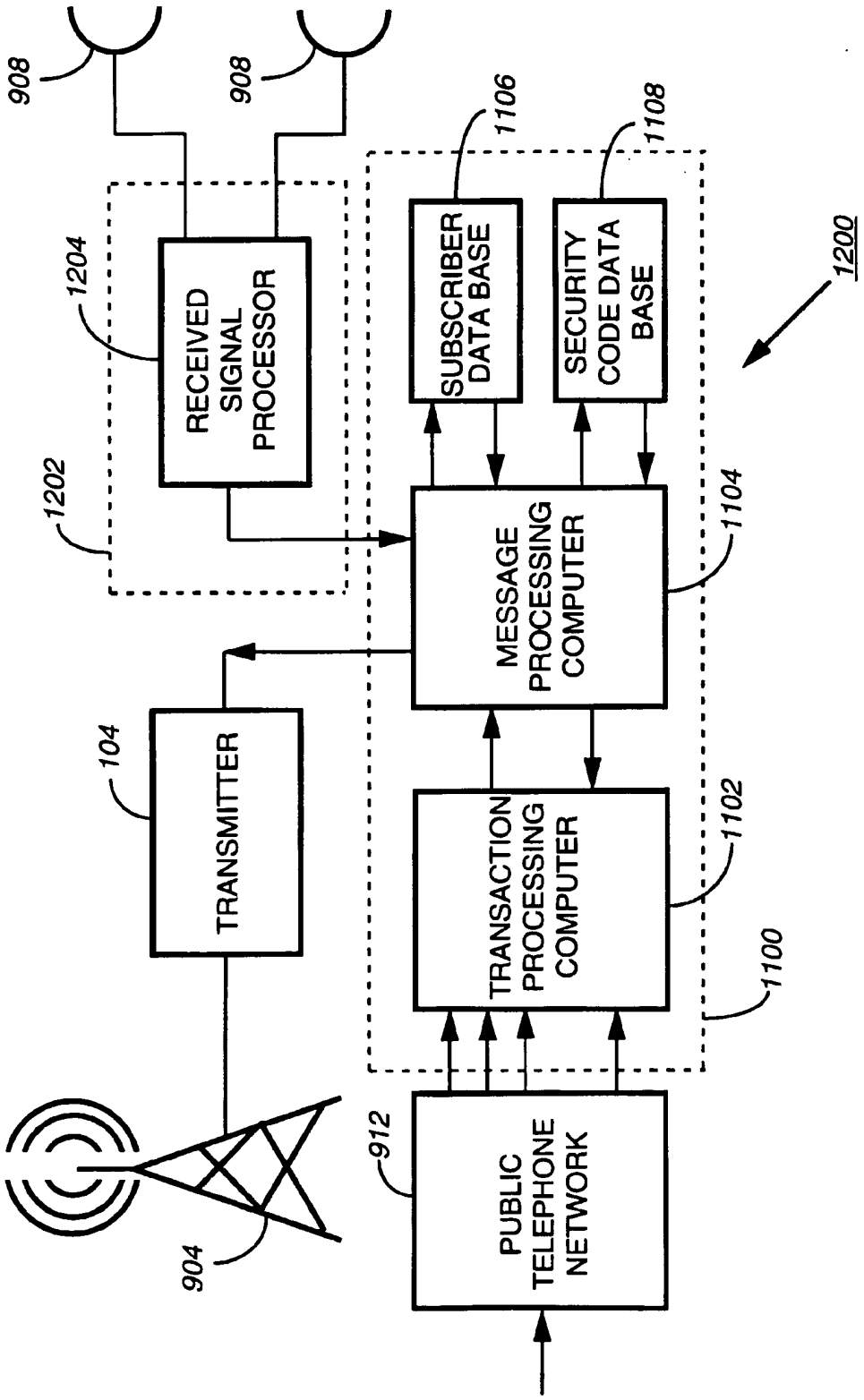

908
908
1106
1108
1200
1204
RECEIVED SIGNAL PROCESSOR
SUBSCRIBER DATA BASE
SECURITY CODE DATA BASE
1202
MESSAGE PROCESSING COMPUTER
1104
104
TRANSMITTER
TRANSACTION PROCESSING COMPUTER
1102
1100
912
PUBLIC TELEPHONE NETWORK
904

FIG. 12

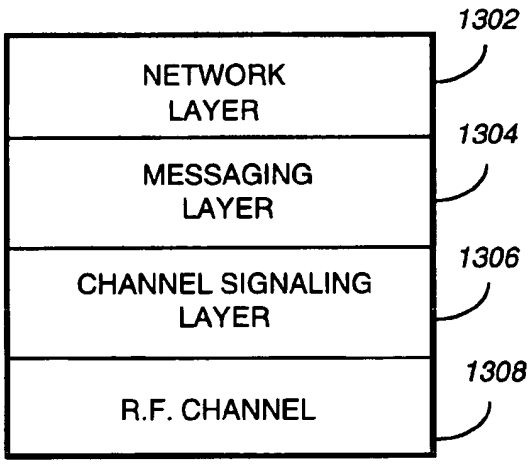

1302
NETWORK LAYER
1304
MESSAGING LAYER
1306
CHANNEL SIGNALING LAYER
1308
R.F. CHANNEL

FIG. 13

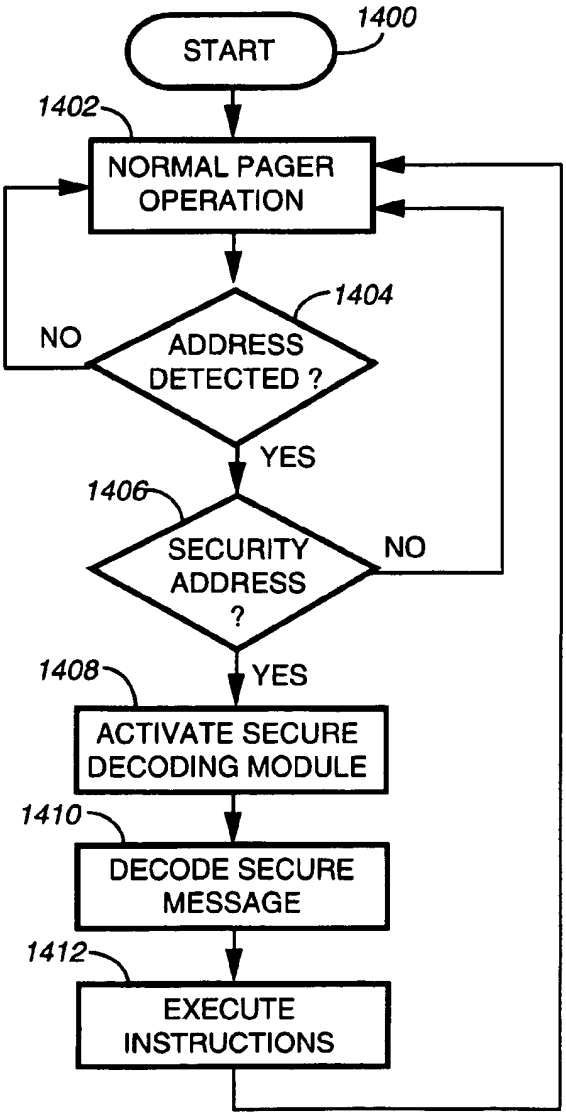

1400
START
1402
NORMAL PAGER OPERATION
1404
ADDRESS DETECTED ?
NO
YES
1406
SECURITY ADDRESS ?
NO
YES
1408
ACTIVATE SECURE DECODING MODULE
1410
DECODE SECURE MESSAGE
1412
EXECUTE INSTRUCTIONS

FIG. 14

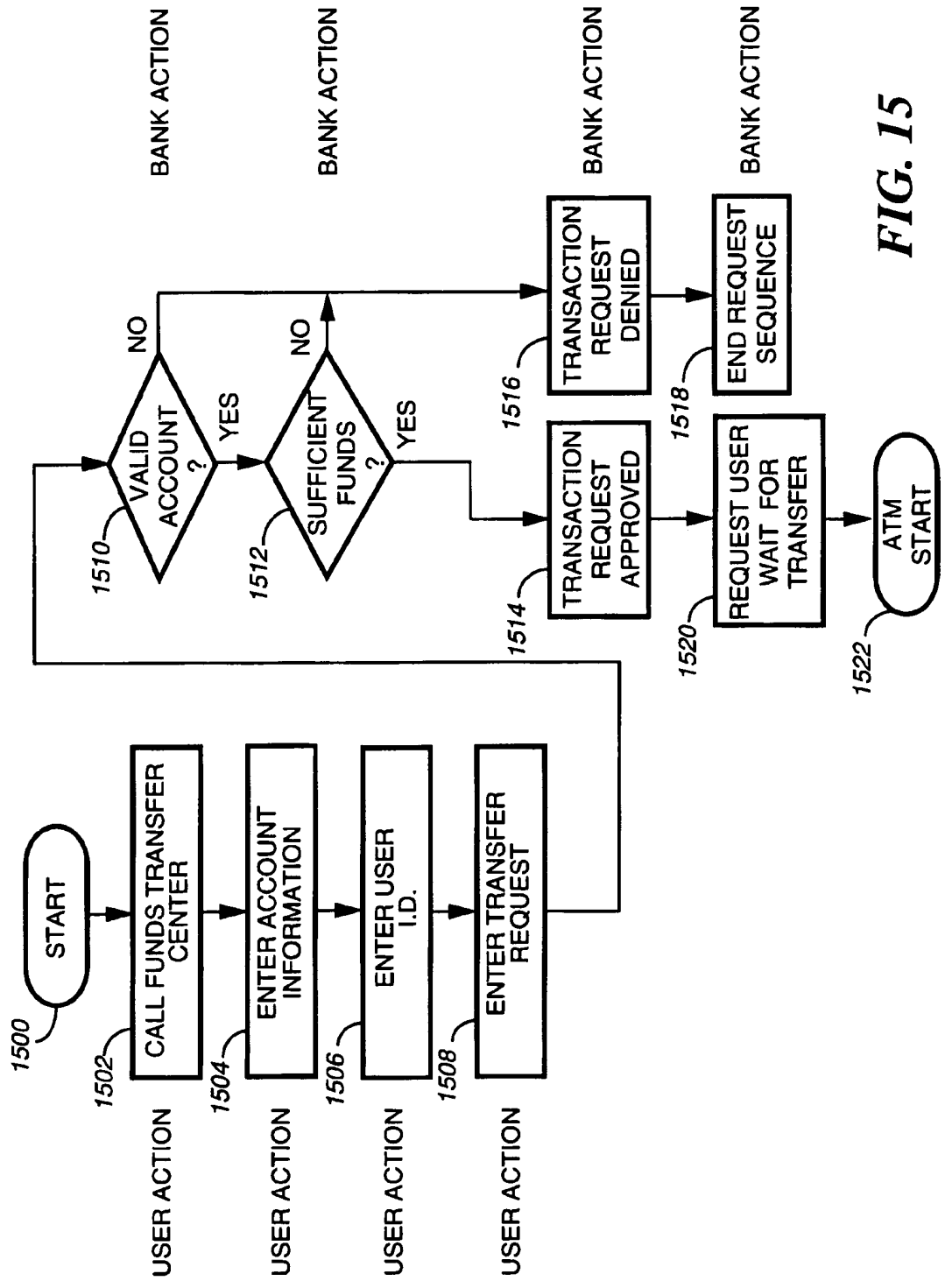

START
1500
CALL FUNDS TRANSFER CENTER
1502
ENTER ACCOUNT INFORMATION
1504
ENTER USER I.D.
1506
ENTER TRANSFER REQUEST
1508
USER ACTION
USER ACTION
USER ACTION
USER ACTION
VALID ACCOUNT ?
1510
NO
YES
SUFFICIENT FUNDS ?
1512
NO
YES
BANK ACTION
BANK ACTION
TRANSACTION REQUEST APPROVED
1514
TRANSACTION REQUEST DENIED
1516
END REQUEST SEQUENCE
1518
REQUEST USER WAIT FOR TRANSFER
1520
ATM START
1522
BANK ACTION
BANK ACTION

FIG. 15

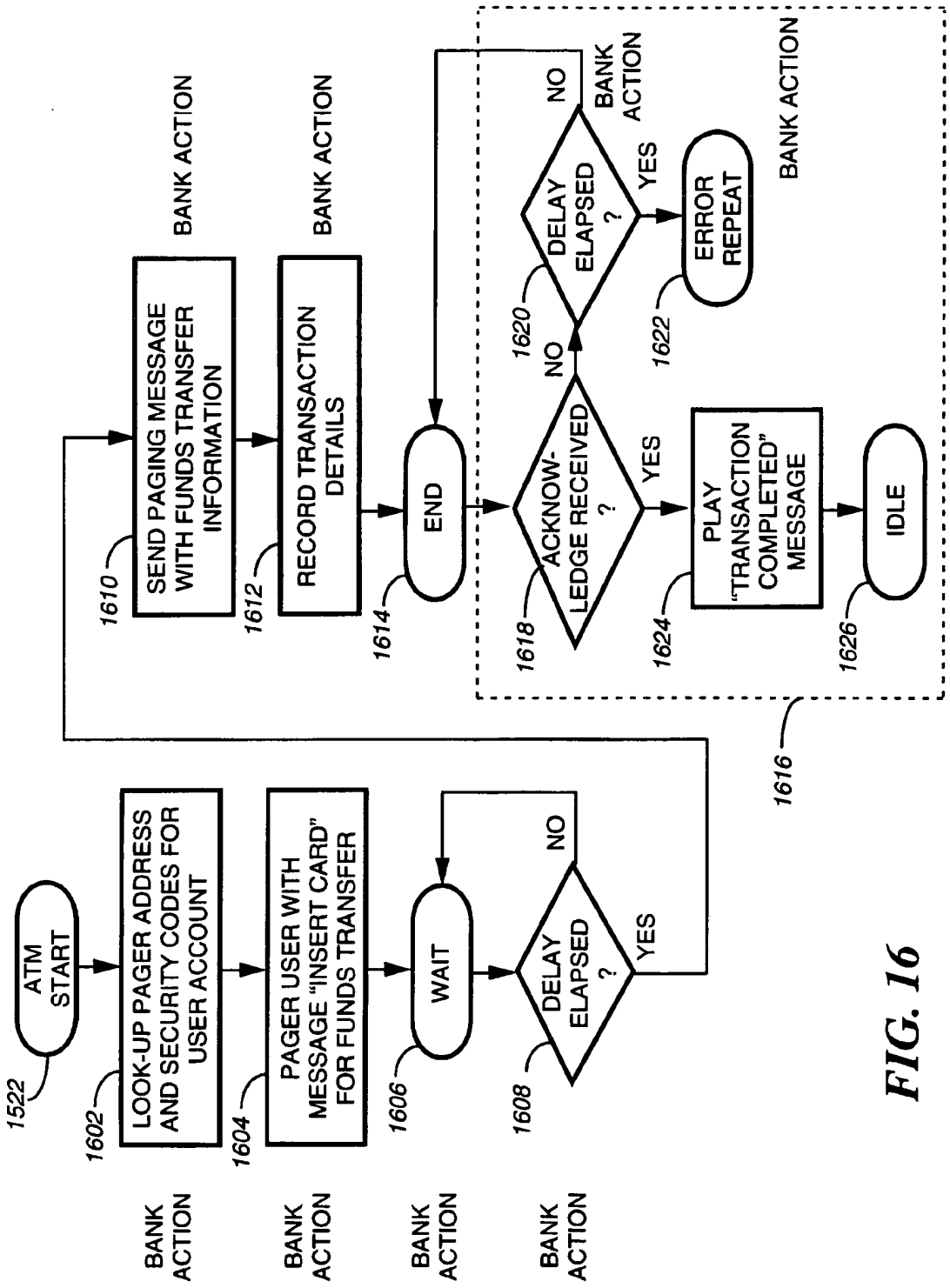

ATM START
1522
LOOK-UP PAGER ADDRESS AND SECURITY CODES FOR USER ACCOUNT
1602
PAGER USER WITH MESSAGE "INSERT CARD" FOR FUNDS TRANSFER
1604
WAIT
1606
DELAY ELAPSED ?
1608
NO
YES
SEND PAGING MESSAGE WITH FUNDS TRANSFER INFORMATION
1610
RECORD TRANSACTION DETAILS
1612
END
1614
ACKNOW-LEDGE RECEIVED ?
1618
NO
YES
DELAY ELAPSED ?
1620
NO
YES
ERROR REPEAT
1622
PLAY "TRANSACTION COMPLETED" MESSAGE
1624
IDLE
1626
1616
BANK ACTION
BANK ACTION
BANK ACTION
BANK ACTION
BANK ACTION
BANK ACTION

FIG. 16

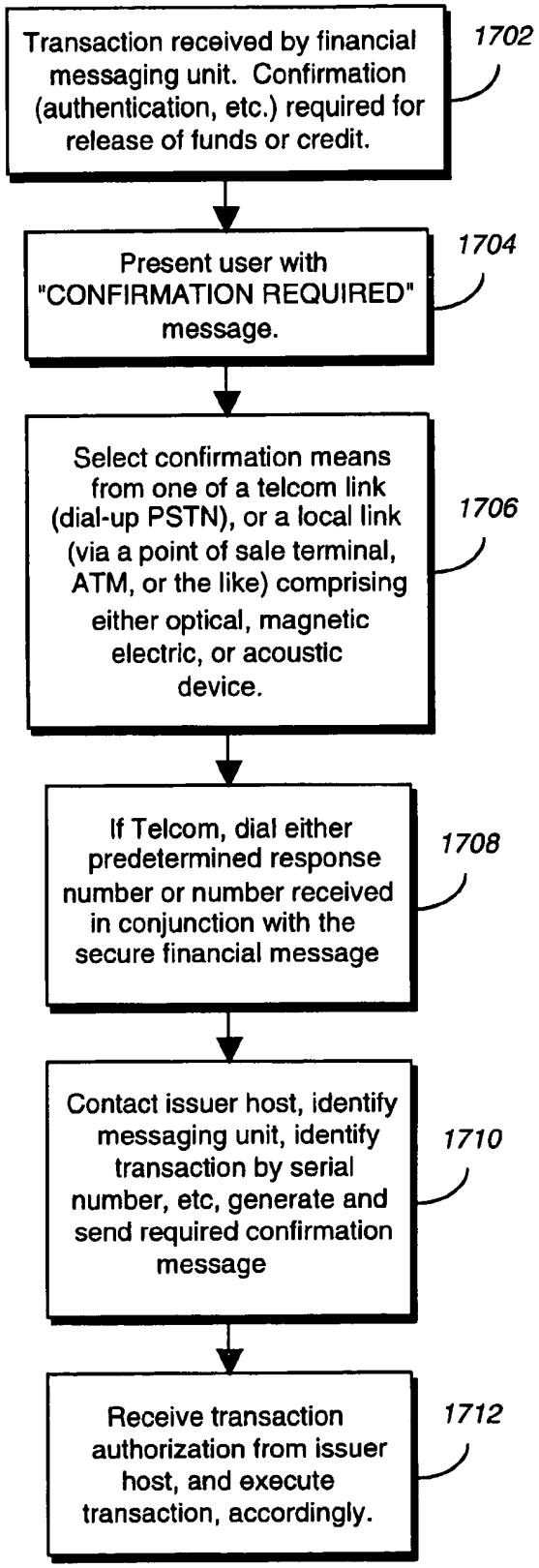

Transaction received by financial messaging unit. Confirmation (authentication, etc.) required for release of funds or credit.
1702
Present user with "CONFIRMATION REQUIRED" message.
1704
Select confirmation means from one of a telcom link (dial-up PSTN), or a local link (via a point of sale terminal, ATM, or the like) comprising either optical, magnetic electric, or acoustic device.
1706
If Telcom, dial either predetermined response number or number received in conjunction with the secure financial message
1708
Contact issuer host, identify messaging unit, identify transaction by serial number, etc, generate and send required confirmation message
1710
Receive transaction authorization from issuer host, and execute transaction, accordingly.
1712

FIG. 17

TRANSACTION AUTHENTICATION FOR 1-WAY WIRELESS FINANCIAL MESSAGING UNITS

FIELD OF THE INVENTION

This invention relates in general to selective call signalling systems and more particularly to a selective call signalling system that facilitates secure financial transactions over a wireless network and an alternate transaction origination and authentication procedure.

BACKGROUND OF THE INVENTION

In conventional selective call signaling systems, a user or originator may send a message to a subscriber unit (e.g., selective call receiver), the message comprising an address associated with the subscriber unit, and data. The data may be in one or more forms such as numeric digits representing a phone number, alphanumeric characters representing a readable text message, or possibly a multimedia message comprising audio and graphical information. Typically, this form of messaging was sufficient to convey information between individuals or services relating to their business, special interests, whereabouts, general scheduling, or time critical appointments. However, because of society's increased need for information when a person is mobile, a solution must be found that allows an individual to perform personal or business transactions, as well as keeping informed of personal events, contacts, and business information.

Considering conventional wireless systems including both cellular and paging applications, there are significant problems that must be solved before reliable and private personal or business transactions can be implemented. Because of the advancement of the engineering sciences, particularly in the areas of wireless communications and computer science, it has become relatively easy for a "hacker" to monitor both the address and data broadcast to the selective call receiver. This unwanted monitoring or eavesdropping poses a problem to potential users of wireless communication systems in that their personal data may be exposed to unauthorized individuals, thus creating an unnecessary risk for both parties if confidential information is broadcast. Moreover, if the information contains clear-text data representing a personal address, serial number Personal Identification Number (PIN) or the like, an unscrupulous party monitoring the data stream could gain access to an individual's personal accounts or pirate the address to clone an unauthorized communication device. The theft of service or confidential information in this manner is probably the most daunting issue facing communication equipment manufacturers and service providers today and in the future. The interest in securing data contained in broadcasts is especially keen in the area of electronic financial transactions. To expose for capture, the clear text data contained in a financial transaction invites, and will surely result, in a theft of funds or fraud against an individual.

Thus, what is needed is wireless messaging system that allows an originator to communicate a secure message between a subscriber unit and the originator, and authenticate the secure message, without exposing the content or meaning of the message.

SUMMARY OF THE INVENTION

Briefly, according to the invention, there is provided a method and apparatus for sending data comprising secure financial transactions over existing paging infrastructure equipment, using paging protocols such as FLEX®, a registered United States trademark of Motorola, Inc., POCSAG (Post Office Code Standardisation Advisory Group), or the like.

A first aspect of the invention involves realizing hardware that implements a method for overlaying secure messaging on an existing paging infrastructure. The existing paging infrastructure comprises a paging terminal that includes a paging encoder for processing received messages and their corresponding destination requests. The paging terminal generates a messaging queue of selective call messages comprising the received messages and their corresponding selective call address(es), as determined from the corresponding destination requests. Distribution of the selective call messages in the messaging queue is handled by the paging terminal which dispatches messages to at least one base station (e.g., transmitter, antenna, and receiver) for communication between the base station and the subscriber unit(s) or pagers.

A second aspect of the invention involves the inclusion of a cryptographic engine in the paging terminal for selectively ciphering, deciphering, signing, and verifying the authenticity of messages received from both an originator and from the subscriber unit or pager.

A third aspect of the invention involves the subscriber unit or pager that is equipped with a special security module that can process cryptographic information contained in the selective call messages to verify their authenticity extract the ciphered data, and return ciphered responses or acknowledgments as necessary, to authenticate and confirm reception of the secure message.

A fourth aspect of the invention involves the subscriber unit or pager being equipped with a primary and possibly a secondary apparatus for communicating both inbound and outbound messages. The primary apparatus comprises a conventional radio frequency receiver and optionally a conventional radio frequency transmitter. The secondary apparatus comprises an optical receiver and optionally an optical transmitter. Alternatively, the secondary apparatus may further comprise one or more acoustic or other electromagnetic transducers and associated circuitry implementing a uni- or bi-directional communication link between the subscriber unit or pager and the originator.

A fifth aspect of the invention involves the subscriber unit or pager including a single, predetermined account identifier corresponding with at least one of an electronic cash or funds storage card, debit card, credit card, or bank account.

A sixth aspect of the invention involves the subscriber unit or pager including multiple predetermined account identifiers corresponding with at least two of the following: electronic cash or funds storage card, debit card, credit card, or bank account.

A seventh aspect of the invention involves the cryptographic engine in the paging terminal and the security module in the subscriber unit or pager accommodating a plurality of cryptographic procedures. These cryptographic procedures comprise both private and public key systems, as appropriate. One such private key system is the Data Encryption Standard (DES) using the ANSI X3.92 DES algorithm in CBC mode. Similarly, a first public key system is RSA (invented by Rivest, Shamir, and Adleman), a cryptographic procedure based on sub-exponential one-way functions implemented using modulo n integer multiplication and exponentation. A second public key system uses elliptic curve technology, a cryptographic procedure based

on highly non-linear exponential one-way functions implemented over finite fields.

An eight aspect of the invention involves initiating a wireless transaction from the subscriber unit or pager, the wireless transaction relating to at least one of the electronic cash or funds storage card, debit card, credit card, or bank account.

A ninth aspect of the invention involves a user selected personal identification number that is programmed into the subscriber unit or pager for protecting financial accounts or funds loaded in the subscriber unit or pager.

A tenth aspect of the invention involves a user selected personal identification number that is programmed into the Smart Card via the subscriber unit or pager, thus disabling access to any features of the protected Smart Card unless subsequently accessed or reprogrammed by the subscriber unit or pager.

An eleventh aspect of the invention involves authenticating the an authorized subscriber unit or pager as a communication agent for the wireless financial transaction, and selectively disallowing any financial transactions directed to accounts belonging to or controlled by the authorized subscriber unit or pager when an inbound or outbound financial transaction is communicated between an issuer and an unauthorized subscriber unit or pager, and in the alternative, preventing fund transfers or credit transactions that exceed a predetermined limit set either by an authorized user or a regulator such as a bank, a credit card issuer or the like.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an electrical block diagram of a data transmission system for use in accordance with the preferred embodiment of the present invention.

FIG. **2** is an electrical block diagram of a terminal for processing and transmitting message information in accordance with the preferred embodiment of the present invention.

FIGS. **3–5** are timing diagrams illustrating the transmission format of the signaling protocol utilized in accordance with the preferred embodiment of the present invention.

FIGS. **6** and **7** are timing diagrams illustrating the synchronization signals utilized in accordance with the preferred embodiment of the present invention.

FIG. **8** is an electrical block diagram of a financial messaging unit in accordance with the preferred embodiment of the present invention.

FIG. **9** is a diagram of a secure messaging system in accordance with the present invention.

FIG. **10** is a high level block diagram of a financial messaging unit in accordance with the preferred embodiment of the present invention.

FIG. **11** is a block diagram of the message composition and encryption equipment that could be used on the premises of a financial institution to send secure electronic funds transfer authorizations to financial messaging units via a paging channel.

FIG. **12** is a functional diagram of a wireless selective call signaling system controller that implements a combined 1-way and 2-way secure messaging system capable of signalling the financial messaging units.

FIG. **13** depicts the various layers of a messaging system in a format that is similar to the Organization Standards International (OSI) stack diagram that is well known in the electronics industry.

FIG. **14** is a flow diagram depicting typical operation of a financial messaging unit in accordance with the preferred embodiment of the present invention.

FIG. **15** illustrates a typical sequence associated with requesting and authorizing the electronic transfer of funds or debit of funds by and from a wireless financial messaging unit.

FIG. **16** illustrates a typical sequence associated with the wireless transfer of funds or debit of funds by and from a wireless financial messaging unit in both a 1-way and a 2-way secure communication system.

FIG. **17** is a flow diagram depicting a typical sequence associated with either authentication or confirmation of a wireless transfer of funds, debit of funds, or credit transaction between a wireless financial messaging unit and a regulator in either a 1-way or a 2-way secure communication system.

DESCRIPTION OF A PREFERRED EMBODIMENT

Referring to FIG. 1, an electrical block diagram illustrates a data transmission system **100**, such as a paging system, for use in accordance with the preferred embodiment of the present invention. In the data transmission system **100**, messages originating either from a phone, as in a system providing numeric data transmission, or from a message entry device, such as an alphanumeric data terminal, are routed through the public switched telephone network (PSTN) to a paging terminal **102** which processes the numeric or alphanumeric message information for transmission by one or more transmitters **104** provided within the system. When multiple transmitters are utilized, the transmitters **104** preferably simulcast transmit the message information to financial messaging units **106**. Processing of the numeric and alphanumeric information by the paging terminal **102**, and the protocol utilized for the transmission of the messages is described below.

Referring to FIG. **2**, an electrical block diagram illustrates the paging terminal **102** utilized for processing and controlling the transmission of the message information in accordance with the preferred embodiment of the present invention. Short messages, such as tone-only and numeric messages which can be readily entered using a Touch-Tone™ telephone are coupled to the paging terminal **102** through a telephone interface **202** in a manner well known in the art. Longer messages, such as alphanumeric messages which require the use of a data entry device are coupled to the paging terminal **102** through a modem **206** using any of a number of well known modem transmission protocols. When a call to place a message is received, a controller **204** handles the processing of the message. The controller **204** is preferably a microcomputer, such as a MC680x0 or equivalent, which is manufactured by Motorola Inc., and which runs various pre-programmed routines for controlling such terminal operations as voice prompts to direct the caller to enter the message, or the handshaking protocol to enable reception of messages from a data entry device. When a call is received, the controller **204** references information stored in the subscriber database **208** to determine how the message being received is to be processed. The subscriber data base **208** includes, but is not limited to such information as addresses assigned to the financial messaging unit, message type associated with the address, and information related to the status of the financial messaging unit, such as active or inactive for failure to pay the bill. A data entry terminal **240** is provided which couples to the controller **204**, and which

is used for such purposes as entry, updating and deleting of information stored in the subscriber data base **208**, for monitoring system performance, and for obtaining such information as billing information.

The subscriber database **208** also includes such information as to what transmission frame and to what transmission phase the financial messaging unit is assigned, as will be described in further detail below. The received message is stored in an active page file **210** which stores the messages in queues according to the transmission phase assigned to the financial messaging unit. In the preferred embodiment of the present invention, four phase queues are provided in the active page file **210**. The active page file **210** is preferably a dual port, first in first out random access memory, although it will be appreciated that other random access memory devices, such as hard disk drives, can be utilized as well. Periodically the message information stored in each of the phase queues is recovered from the active page file **210** under control of controller **204** using timing information such as provided by a real time clock **214**, or other suitable timing source. The recovered message information from each phase queue is sorted by frame number and is then organized by address, message information, and any other information required for transmission (all of which is referred to as message related information), and then batched into frames based upon message size by frame batching controller **212**. The batched frame information for each phase queue is coupled to frame message buffers **216** which temporarily store the batched frame information until a time for further processing and transmission. Frames are batched in numeric sequence, so that while a current frame is being transmitted, the next frame to be transmitted is in the frame message buffer **216**, and the next frame thereafter is being retrieved and batched. At the appropriate time, the batched frame information stored in the frame message buffer **216** is transferred to the frame encoder **218**, again maintaining the phase queue relationship. The frame encoder **218** encodes the address and message information into address and message codewords required for transmission, as will be described below. The encoded address and message codewords are ordered into blocks and then coupled to a block interleaver **220** which interleaves preferably eight codewords at a time to form interleaved information blocks for transmission in a manner well known in the art. The interleaved codewords contained in the interleaved information blocks produced by each block interleaver **220** are then serially transferred to a phase multiplexer **221**, which multiplexes the message information on a bit by bit basis into a serial data stream by transmission phase. The controller **204** next enables a frame sync generator **222** which generates the synchronization code which is transmitted at the start of each frame transmission. The synchronization code is multiplexed with address and message information under the control of controller **204** by serial data splicer **224**, and generates therefrom a message stream which is properly formatted for transmission. The message stream is next coupled to a transmitter controller **226**, which under the control of controller **204** transmits the message stream over a distribution channel **228**. The distribution channel **228** may be any of a number of well known distribution channel types, such as wire line, an RF or microwave distribution channel, or a satellite distribution link. The distributed message stream is transferred to one or more transmitter stations **104**, depending upon the size of the communication system. The message stream is first transferred into a dual port buffer **230** which temporarily stores the message stream prior to transmission. At an appropriate time determined by timing and control circuit **232**, the message stream is recovered from the dual port buffer **230** and coupled to the input of preferably a 4-level FSK modulator **234**. The modulated message stream is then coupled to the transmitter **236** for transmission via antenna **238**.

Referring to FIGS. **3**, **4** and **5**, the timing diagrams illustrate the transmission format of the signaling protocol utilized in accordance with the preferred embodiment of the present invention. This signalling protocol is commonly referred to as Motorola's FLEX selective call signalling protocol. As shown in FIG. **3**, the signaling protocol enables message transmission to financial messaging units, such as pagers, assigned to one or more of 128 frames which are labeled frame 0 through frame 127. It then will be appreciated that the actual number of frames provided within the signaling protocol can be greater or less than described above. The greater the number of frames utilized, the greater the battery life that may be provided to the financial messaging units operating within the system. The fewer the number of frames utilized, the more often messages can be queued and delivered to the financial messaging units assigned to any particular frame thereby reducing the latency, or time required to deliver messages.

As shown in FIG. **4**, the frames comprise a synchronization codeword (sync) followed preferably by eleven blocks of message information (information blocks) which are labeled block 0 through block 10. As shown in FIG. **5**., each block of message information comprises preferably eight address, control or data codewords which are labeled word 0 through word 7 for each phase. Consequently, each phase in a frame allows the transmission of up to eighty-eight address, control and data codewords. The address, control and data codewords preferably comprise two sets, a set first relating to a vector field comprising a short address vector, a long address vector, a first message word, and a null word, and a second set relating to a message field comprising a message word and a null word.

The address, control, and data or message codewords are preferably 31,21 BCH codewords with an added thirty-second even parity bit which provides an extra bit of distance to the codeword set. It will be appreciated that other codewords, such as a 23,12 Golay codeword could be utilized as well. Unlike the well known POCSAG signaling protocol which provides address and data codewords which utilize the first codeword bit to define the codeword type, as either address or data, no such distinction is provided for the address and data codewords in the FLEX signaling protocol utilized with the preferred embodiment of the present invention. Rather, address and data codewords are defined by their position within the individual frames.

FIGS. **6** and **7** are timing diagrams illustrating the synchronization code utilized in accordance with the preferred embodiment of the present invention. In particular, as shown in FIG. **6**, the synchronization code comprises preferably three parts, a first synchronization code (sync 1), a frame information codeword (frame info) and a second synchronization codeword (sync 2). As shown in FIG. **7**, the first synchronization codeword comprises first and third portions, labeled bit sync 1 and BS1, which are alternating 1,0 bit patterns which provides bit synchronization, and second and fourth portions, labeled "A" and its complement "A bar", which provide frame synchronization. The second and fourth portions are preferably single 32,21 BCH codewords which are predefined to provide high codeword correlation reliability, and which are also used to indicate the data bit rate at which addresses and messages are transmitted. Table

1 defines the data bit rates which are used in conjunction with the signaling protocol.

TABLE 1

Bit Rate	"A" Value
1600 bps	A1 and A1 bar
3200 bps	A2 and A2 bar
6400 bps	A3 and A3 bar
Not defined	A4 and A4 bar

As shown in Table 1, three data bit rates are predefined for address and message transmission, although it will be appreciated that more or less data bit rates can be predefined as well, depending upon the system requirements.

The frame information codeword is preferably a single 32,21 BCH codeword which includes within the data portion a predetermined number of bits reserved to identify the frame number, such as 7 bits encoded to define frame number 0 to frame number 127.

The structure of the second synchronization code is preferably similar to that of the first synchronization code described above. However, unlike the first synchronization code which is preferably transmitted at a fixed data symbol rate, such as 1600 bps (bits per second), the second synchronization code is transmitted at the data symbol rate at which the address and messages are to be transmitted in any given frame. Consequently, the second synchronization code allows the financial messaging unit to obtain "fine" bit and frame synchronization at the frame transmission data bit rate.

In summary the signaling protocol utilized with the preferred embodiment of the present invention comprises 128 frames which include a predetermined synchronization code followed by eleven information blocks which comprise eight address, control or message codewords per phase. The synchronization code enables identification of the data transmission rate, and insures synchronization by the financial messaging unit with the data codewords transmitted at the various transmission rates.

FIG. **8** is an electrical block diagram of the financial messaging unit **106** in accordance with the preferred embodiment of the present invention. The heart of the financial messaging unit **106** is a controller **816**, which is preferably implemented using a low power MC68HC0x microcomputer, such as manufactured by Motorola, Inc., or the like. The microcomputer controller, hereinafter call the controller **816**, receives and processes inputs from a number of peripheral circuits, as shown in FIG. **8**, and controls the operation and interaction of the peripheral circuits using software subroutines. The use of a microcomputer controller for processing and control functions (e.g., as a function controller) is well known to one of ordinary skill in the art.

The financial messaging unit **106** is capable of receiving address, control and message information, hereafter called "data" which is modulated using preferably 2-level and 4-level frequency modulation techniques. The transmitted data is intercepted by an antenna **802** which couples to the input of a receiver section **804**. Receiver section **804** processes the received data in a manner well known in the art, providing at the output an analog 4-level recovered data signal, hereafter called a recovered data signal. The recovered data signal is coupled to one input of a threshold level extraction circuit **808**, and to an input of a 4-level decoder **810**.

Operation of the threshold level extraction circuit **808**, 4-level decoder **810**, symbol synchronizer **812**, 4-level to binary converter **814**, synchronization codeword correlator **818**, and phase timing generator (data recovery timing circuit) **826** depicted in the financial messaging unit of FIG. **8** is best understood with reference to U.S. Pat. No. 5,282,205 entitled "Data Communication Terminal Providing Variable Length Message Carry-On And Method Therefor," issued to Kuznicki et al., assigned to Motorola, Inc., the teachings of which are incorporated herein by reference thereto.

Again referring to FIG. **8**, the threshold level extraction circuit **808** comprises two clocked level detector circuits (not shown) which have as inputs the recovered data signal. Preferably, signal states of 17%, 50% and 83%, are utilized to enable decoding the 4-level data signals presented to the threshold level extraction circuit **808**.

When power is initially applied to the receiver portion, as when the financial messaging unit is first turned on, a clock rate selector is preset through a control input (center sample) to select a 128× clock, i.e. a clock having a frequency equivalent to 128 times the slowest data bit rate, which as described above is 1600 bps. The 128× clock is generated by 128× clock generator **844**, as shown in FIG. **8**, which is preferably a crystal controlled oscillator operating at 204.8 KHz (kilohertz). The output of the 128× clock generator **844** couples to an input of frequency divider **846** which divides the output frequency by two to generate a 64× clock at 102.4 KHz. The 128× clock allows the level detectors to asynchronously detect in a very short period of time the peak and valley signal amplitude values, and to therefore generate the low (Lo), average (Avg) and high (Hi) threshold output signal values required for modulation decoding. After symbol synchronization is achieved with the synchronization signal, as will be described below, the controller **816** generates a second control signal (center sample) to enable selection of a 1× symbol clock which is generated by symbol synchronizer **812** as shown in FIG. **8**.

The 4-level decoder **810** preferably operates using three voltage comparators and a symbol decoder. The recovered data signal is coupled to an input of the three comparators having thresholds corresponding with normalized signal states of 17%, 50% and 83%. The resulting system effectively recovers the demodulated 2- or 4-level FSK information signal by coupling the recovered data signal to the second input of an 83% comparator, the second input of a 50% comparator, and the second input of a 17% comparator. The outputs of the three comparators corresponding with the low (Lo), average (Avg) and high (Hi) threshold output signal values are coupled to inputs of a symbol decoder. The symbol decoder then decodes the inputs according to Table 2.

TABLE 2

Threshold			Output	
Hi	Avg	Lo	MSB	LSB
RC_{in} <	RC_{in} <	RC_{in} <	0	0
RC_{in} <	RC_{in} <	RC_{in} >	0	1
RC_{in} <	RC_{in} >	RC_{in} >	1	1
RC_{in} >	RC_{in} >	RC_{in} >	1	0

As shown in Table 2, when the recovered data signal (RC_{in}) is less than all three threshold values, the symbol generated is 00 (MSB=0, LSB=0). Thereafter, as each of the three threshold values is exceeded, a different symbol is generated, as shown in the table above.

The MSB output from the 4-level decoder **810** is coupled to an input of the symbol synchronizer **812** and provides a

recovered data input generated by detecting the zero crossings in the 4-level recovered data signal. The positive level of the recovered data input represents the two positive deviation excursions of the analog 4-level recovered data signal above the average threshold output signal, and the negative level represents the two negative deviation excursions of the analog 4-level recovered data signal below the average threshold output signal.

The symbol synchronizer **812** uses a 64× clock at 102.4 KHz which is generated by frequency divider **846**, that is coupled to an input of a 32× rate selector (not shown). The 32× rate selector is preferably a divider which provides selective division by 1 or 2 to generate a sample clock which is thirty-two times the symbol transmission rate. A control signal (1600/3200) is coupled to a second input of the 32× rate selector, and is used to select the sample clock rate for symbol transmission rates of 1600 and 3200 symbols per second. The selected sample clock is coupled to an input of 32× data oversampler (not shown) which samples the recovered data signal (MSB) at thirty-two samples per symbol. The symbol samples are coupled to an input of a data edge detector (not shown) which generates an output pulse when a symbol edge is detected. The sample clock is also coupled to an input of a divide-by-16/32 circuit (not shown) which is utilized to generate 1× and 2× symbol clocks synchronized to the recovered data signal. The divided-by-16/32 circuit is preferably an up/down counter. When the data edge detector detects a symbol edge, a pulse is generated which is gated by an AND gate with the current count of divide-by-16/32 circuit. Concurrently, a pulse is generated by the data edge detector which is also coupled to an input of the divide-by-16/32 circuit. When the pulse coupled to the input of the AND gate arrives before the generation of a count of thirty-two by the divide-by-16/32 circuit, the output generated by the AND gate causes the count of divide-by-16/32 circuit to be advanced by one count in response to the pulse which is coupled to the input of divide-by-16/32 circuit from the data edge detector, and when the pulse coupled to the input of the AND gate arrives after the generation of a count of thirty-two by the divide-by-16/32 circuit, the output generated by the AND gate causes the count of divide-by-16/32 circuit to be retarded by one count in response to the pulse which is coupled to the input of divide-by-16/32 circuit from the data edge detector, thereby enabling the synchronization of the 1× and 2× symbol clocks with the recovered data signal. The symbol clock rates generated are best understood from Table 3 below.

TABLE 3

Input Clock (Relative)	Control Input (SPS)	Rate Selector Divide Ratio	Rate Selector Output	2X Symbol Clock (BPS)	1X Symbol Clock (BPS)
64X	1600	by 2	32X	3200	1600
64X	3200	by 1	64X	6400	3200

As shown in the table above, the 1× and 2× symbol clocks are generated 1600, 3200 and 6400 bits per second and are synchronized with the recovered data signal.

The 4-level binary converter **814** couples the 1× symbol clock to a first clock input of a clock rate selector (not shown). A 2× symbol clock is coupled to a second clock input of the clock rate selector. The symbol output signals (MSB, LSB) are coupled to inputs of an input data selector (not shown). A selector signal (2L/4L) is coupled to a selector input of the clock rate selector and the selector input of the input data selector, and provides control of the conversion of the symbol output signals as either 2-level FSK data, or 4-level FSK data. When the 2-level FSK data conversion (2L) is selected, only the MSB output is selected which is coupled to the input of a conventional parallel to serial converter (not shown). The 1× clock input is selected by clock rate selector which results in a single bit binary data stream to be generated at the output of the parallel to serial converter. When the 4-level FSK data conversion (4L) is selected, both the LSB and MSB outputs are selected which are coupled to the inputs of the parallel to serial converter. The 2× clock input is selected by clock rate selector which results in a serial two bit binary data stream to be generated at 2× the symbol rate, which is provided at the output of the parallel to serial converter.

Referring again to FIG. **8**, the serial binary data stream generated by the 4-level to binary converter **814** is coupled to inputs of a synchronization codeword correlator **818** and a demultiplexer **820**. Predetermined "A" codeword synchronization patterns are recovered by the controller **816** from a code memory **822** and are coupled to an "A" codeword correlator (not shown). When the synchronization pattern received matches one of the predetermined "A" codeword synchronization patterns within an acceptable margin of error, an "A" or "A-bar" output is generated and is coupled to controller **816**. The particular "A" or "A-bar" codeword synchronization pattern correlated provides frame synchronization to the start of the frame ID codeword, and also defines the data bit rate of the message to follow, as was previously described.

The serial binary data stream is also coupled to an input of the frame codeword decoder (not shown) which decodes the frame codeword and provides an indication of the frame number currently being received by the controller **816**. During sync acquisition, such as following initial receiver turn-on, power is supplied to the receiver portion by battery saver circuit **848**, shown in FIG. **8**, which enabled the reception of the "A" synchronization codeword, as described above, and which continues to be supplied to enable processing of the remainder of the synchronization code. The controller **816** compares the frame number currently being received with a list of assigned frame numbers stored in code memory **822**. Should the currently received frame number differ from an assigned frame numbers, the controller **816** generates a battery saving signal which is coupled to an input of battery saver circuit **848**, suspending the supply of power to the receiver portion. The supply of power will be suspended until the next frame assigned to the receiver, at which time a battery saver signal is generated by the controller **816** which is coupled to the battery saving circuit **848** to enable the supply of power to the receiver portion to enable reception of the assigned frame.

A predetermined "C" codeword synchronization pattern is recovered by the controller **816** from a code memory **822** and is coupled to a "C" codeword correlator (not shown). When the synchronization pattern received matches the predetermined "C" codeword synchronization pattern with an acceptable margin of error, a "C" or "C-bar" output is generated which is coupled to controller **816**. The particular "C" or "C-bar" synchronization codeword correlated provides "fine" frame synchronization to the start of the data portion of the frame.

The start of the actual data portion is established by the controller **816** generating a block start signal (Blk Start) which is coupled to inputs of a codeword de-interleaver **824** and a data recovery timing circuit **826**. A control signal (2L/4L) is coupled to an input of clock rate selector (not

shown) which selects either 1× or 2× symbol clock inputs. The selected symbol clock is coupled to the input of a phase generator (not shown) which is preferably a clocked ring counter which is clocked to generate four phase output signals (Ø1–Ø4). A block start signal is also coupled to an input of the phase generator, and is used to hold the ring counter in a predetermined phase until the actual decoding of the message information is to begin. When the block start signal releases the phase generator, it begins generating clocked phase signals which are synchronized with the incoming message symbols.

The clocked phase signal outputs are then coupled to inputs of a phase selector **828**. During operation, the controller **816** recovers from the code memory **822**, the transmission phase number to which the financial messaging unit is assigned. The phase number is transferred to the phase select output (Ø Select) of the controller **816** and is coupled to an input of phase selector **828**. A phase clock, corresponding to the transmission phase assigned, is provided at the output of the phase selector **828** and is coupled to clock inputs of the demultiplexer **820**, block de-interleaver **824**, and address and data decoders **830** and **832**, respectively. The demultiplexer **820** is used to select the binary bits associated with the assigned transmission phase which are then coupled to the input of block de-interleaver **824**, and clocked into the de-interleaver array on each corresponding phase clock. In a first embodiment, the de-interleaver uses an 8×32 bit array which de-interleaves eight 32 bit interleaved address, control or message codewords, corresponding to one transmitted information block. The de-interleaved address codewords are coupled to the input of address correlator **830**. The controller **816** recovers the address patterns assigned to the financial messaging unit, and couples the patterns to a second input of the address correlator. When any of the de-interleaved address codewords matches any of the address patterns assigned to the financial messaging unit within an acceptable margin of error (e.g., the number of bit errors correctable according to the codeword structure selected), the message information and corresponding information associated with the address (e.g., the information representing the broadcast and received selective call signalling message, which was previously defined as message related information) is then decoded by the data decoder **832** and stored in a message memory **850**.

Following the detection of an address associated with the financial messaging unit, the message information is coupled to the input of data decoder **832** which decodes the encoded message information into preferably a BCD or ASCII format suitable for storage and subsequent display.

Alternatively, the software based signal processor may be replaced with a hardware equivalent signal processor that recovers the address patterns assigned to the financial messaging unit, and the message related information. Following, or prior to detection of an address associated with the financial messaging unit, the message information and corresponding information associated with the address may be stored directly in the message memory **850**. Operation in this manner allows later decoding of the actual message information, e.g., that encoded message information that decodes into a BCD, ASCII; or multimedia format suitable for subsequent presentation. However, in performing direct storage, the memory must be structured in a manner that allows efficient, high speed placement of the message information and corresponding information associated with the address. Additionally, to facilitate the direct storage of message information and corresponding information associated with the address in the message memory **850**, a codeword identifier **852** examines the received codeword to assign a type identifier to the codeword in response to the codeword belonging to one of a set comprising a vector field and a set comprising a message field. After determining the type identifier, a memory controller **854** operates to store the type identifier in a second memory region within the memory corresponding with the codeword. The above memory structure and operation of the de-interleaved information memory storage device comprising the message memory **850**, the codeword identifier **852**, and the memory controller **854**, are more fully discussed in the patents incorporated below.

Following the storage of the message related information, a sensible alert signal is generated by the controller **816**. The sensible alert signal is preferably an audible alert signal, although it will be appreciated that other sensible alert signals, such as tactile alert signals, and visual alert signals can be generated as well. The audible alert signal is coupled by the controller **816** to an alert driver **834** which is used to drive an audible alerting device, such as a speaker or a transducer **836**. The user can override the alert signal generation through the use of user input controls **838** in a manner well known in the art.

The stored message information can be recalled by the user using the user input controls **838** whereupon the controller **816** recovers the message information from memory, and provides the message information to a display driver **840** for presentation on a display **842**, such as an LCD display.

In addition to the preceding description, the systems previously discussed in reference to FIGS. **1, 2, 7** and **8**, and protocol previously discussed in reference to FIGS. **3, 4** and **5** may be more fully understood in view of the following U.S. Pat. No. 5,168,493 entitled "Time Division Multiplexed Selective Call System" issued to Nelson et al., U.S. Pat. No. 5,371,737 entitled "Selective Call Receiver For Receiving A Multiphase Multiplexed Signal" issued to Nelson et al., U.S. Pat. No. 5,128,665 entitled "Selective Call Signalling System" to DeLuca et al., and U.S. Pat. No. 5,325,088 entitled "Synchronous Selective Signalling System" to Willard et al., all of which are assigned to Motorola, Inc., and the teachings of which are incorporated herein by reference thereto.

Referring to FIG. **9**, a diagram shows a secure messaging system **900** in accordance with the present invention.

The paging terminal **102** or wireless selective call signalling system controller, receives information comprising a selective call message request including a destination identifier and a secure financial transaction message. The information is typically coupled to the paging terminal **102** via a Public Switched Telephone Network (PSTN) **912** which serves to transport the information from a regulator **914** such as a bank, credit card issuer or the like. The PSTN **912** may be coupled to the paging terminal **102** and the regulator **914** using conventional phone lines **910** or possibly a high speed digital network, depending on the information bandwidth required for communicating financial transactions between the regulator **914** and a plurality of one financial messaging unit **906**. Once coupled to the paging terminal **102**, the information is formatted as one or more selective call messages and transferred **922** to at least one radio frequency transmitter **904** for broadcast to at least one financial messaging unit **906** located in any one of a number of communication zones **902**. The financial messaging unit **906** may include an interface that couples unencrypted or encrypted information such as the secure financial transaction message

to a conventional Smart Card **920** for effecting a financial transaction. Alternatively, the secure financial transaction message may be decoded and stored by the financial messaging unit **906** when the financial messaging unit **906** includes capabilities, e.g., cash load and reload and/or credit services, such as found in a Smart Card **920**.

Two-way capability is provided for the financial messaging unit **906** using either a wired or a wireless return path. By way of example, the secure financial transaction message is received by the financial messaging unit **906** which decodes and decrypts a content of the secure financial transaction message that may represent a cash value token, credit, or debit amount. This message content is then stored by the financial messaging unit **906** pending confirmation of receipt and a subsequent release of funds or authorization of credit by the regulator. If the financial transaction value is high, the regulator will typically require an acknowledgment from the financial messaging unit **906** before the received token based funds are activated, or before a credit or debit transaction is allowed. However, if the financial transaction value is low, the regulator may not require an acknowledgment from the financial messaging unit **906** before the received token based funds are activated, or before a credit or debit transaction is allowed. In case of a low value transaction, the financial messaging unit **906** may only be required to reconcile its fund or credit capacity one a day, or week.

The secure messaging system illustrated in FIG. **9** allows wireless return or origination of secure financial transaction messages using a reverse or inbound channel received by distributed receiver sites **908**. These sites are typically more dense that the outbound broadcast sites **904** since the transmitter power and antenna characteristics of the financial messaging unit **906** are significantly inferior to that of a dedicated radio frequency base station and wide area transmitter site **904**. Thus, the size and weight of a financial messaging unit **906** is kept to a minimum, yielding a more ergonomic portable device with the value added function of not requiring a physical connection to effect financial transactions such as bank withdrawals, deposits, credit card payments, or purchases. The secure messaging system is preferably designed to accommodate low power secure financial messaging unit **906** that include devices such as a message origination unit **1038** and transducer **1040** for implementing the return or origination of secure financial transaction messages using a reverse or inbound channel **924** that is preferably accessed at a merchant **916**. Such return or origination messages are coupled to a regulator or bank **914** via an Automatic Teller Machine (ATM) **926**, a point of sale terminal **928** or the like. These ATMs point of sale terminals necessarily include transducers with reciprocal properties to those found in the message origination unit **1038**. In these cases, the low power secure financial messaging unit **906** comprises an infrared or laser optical port, a low power proximate magnetic inductive or electric capacitive port, or possibly an acoustic, e.g., ultrasonic or audio band acoustic transducer port, any of which operate couple signals between the lower power secure financial messaging unit **906** and the ATM **926**, the point of sale terminal **928**, or the like. In this way, financial transactions can be effected based on a remote transaction request typically made through a bank **914** or issuer, as well as financial transactions locally requested by a user having a suitable secure financial messaging unit **906**. It is important to note that local, low power origination, confirmation, and authentication carried out by the secure financial messaging unit **906**complements the overall system security since the wireless transmissions are limited in range and dispersion. In particular, transmission by an optical device is line of sight and extremely directional, thus thwarting any unwanted interception by an unauthorized party. Similarly, if an acoustic or low power electromagnetic device is employed for reverse or local channel communications, interception of the communications is difficult due to the limited range and duration of the communications.

Regarding the security of communications, several cryptographic methods are suitable for use with the present invention. The following definitions are useful in understanding the terminology associated with cryptography as applied to wired or wireless communications contemplated for use with the present invention.

Certificate—Certificates are digital documents attesting to the binding of a public key to an individual or other entity. Certificates are issued by a Certification Authority (CA), which can be any trusted central administration willing to vouch for the identities of those to whom it issues certificates. A certificate is created when a CA signs a user's public key plus other identifying information, binding the user to their public key. Users present their certificate to other users to demonstrate the validity of their public keys.

Confidentiality—The result of keeping information secret from all but those who are authorized to see it. Confidentiality is also referred to as privacy.

Cryptographic Protocol—A distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective.

Data Integrity—The assurance that information has not been altered by unauthorized or unknown means.

Decryption—The process of transforming encrypted information (cipher text) into plain text.

DES (Data Encryption Standard)—A symmetric encryption cipher defined and endorsed by the U.S. government as an official standard. It is the most well-known and widely used cryptosystem in the world.

Diffie-Hellman—The Diffie-Hellman key agreement protocol provided the first practical solution to the key distribution problem by allowing parties to securely establish a shared secret key over an open channel. The security is based on the discrete log problem.

Digital Signature—A data string which associations a message (in digital form) with the originating entity. This cryptographic primitive is used to provide authentication, data integrity and non-repudiation.

Discrete Log Problem—The requirement to find the exponent x in the formula $y=g^x \bmod p$. The discrete log problem is believed to be difficult and the hard direction of a one-way function.

Elliptic Curve Cryptosystem (ECC)—A public-key cryptosystem based on the discrete logarithm problem over elliptic curves. ECC provides the highest strength-per-bit of any public-key system, allowing the use of much smaller public-keys compared to other systems.

Encryption—The process of transforming plain text into cipher text for confidentiality or privacy.

Entity Authentication—The corroboration of the identity of an entity (e.g., a person, financial messaging unit, computer terminal, Smart Card, etc.).

Factoring—The act of splitting an integer into a set of smaller integers which, when multiplied together, form the original integer. RSA is based on the factoring of large prime numbers.

Information Security Functions—The processes of encryption and digital signatures which provide information security services. Also known as security primitives.

Information Security Services—The purpose of utilizing information security functions. Services include privacy or confidentiality, authentication, data integrity and non-repudiation.

Key—A value in the form of a data string used by information security functions to perform cryptographic computations.

Key Agreement—A key establishment technique in which a shared secret is derived by two or more parties as a function or information contributed by, or associated with, each of these such that no party can predetermine the resulting value.

Key Establishment—Any process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use.

Key Management—The set of processes and mechanisms which support key establishment and the maintenance of ongoing keying relationships between parties.

Key Pair—The public key and private key of a user or entity in a public-key cryptosystem. Keys in a key pair are mathematically related by a hard one-way function.

Key Transport—A key establishment technique where one party creates or otherwise obtains a secret value and securely transfers it to the other party or parties.

Message Authentication—The corroboration of the source of information; also known as data original authentication.

Message Authentication Code (MAC)—A hash function which involves a secret key, and provides data original authentication and data integrity. The MAC is also referred to as a transaction authentication code, wherein a message may contain at least one transactions.

Non-repudiation—The prevention of the denial of previous commitments or actions. Non-repudiation is achieved using digital signatures.

Private Key—In a public-key system, it is that key in a key pair which is held by the individual entity and never revealed. It is preferable to embed the private key in a hardware platform as a measure to keep it hidden from unauthorized parties.

Public Key—In a public key system, it is that key in a key pair which is made public.

Public-Key Cryptography—A cryptographic system that uses different keys for encryption (e) and decryption (d), where (e) and (d) are mathematically linked. It is computationally infeasible to determine (d) from (e). Therefore, this system allows the distribution of the public key while keeping the private key secret. Public-key cryptography is the most important advancement in the field of cryptography in the last 2000 years.

RSA—A widely used public-key cryptosystem, named after its inventors R. Rivest, A. Shamir, and L. Adleman. The security of RSA is based on the intractability of the integer factorization problem.

Symmetric-Key Encryption—A cryptosystem in which for each associated encryption/decryption key pair, (e,d), it is computationally easy to determine d knowing only e, and to determine e from d. In most practical symmetric-key encryption schemes e=d. Although symmetric systems are efficient for bulk encryption of data, they pose significant key management problems. Consequently, symmetric-key and public-key systems are often combined in a system to take advantage of the benefits of each.

Asymmetric-Key Encryption—A cryptosystem in which for each party holds encryption/decryption key pairs with varying strength, e.g., a shorter key may be used in situations requiring less security, while a longer key is used in situations requiring greater security. As with symmetric-key encryption systems, asymmetric systems pose significant key management problems.

Verification—The process of confirming that a digital signature, and therefore an entity or a message, is authentic.

The following examples illustrate systems that may be used to implement a secure messaging system in accordance with the present invention.

Using ECC Algorithms, a secure signature with hash is generated based on the following information:

P is a generating point on the curve and has order n.

H is a secure hash algorithm such as SHA-1.

M is a bit string to be signed by an entity A

A has a private key a and a public key Y_a=aP.

To generate the signature, Entity A does the following:

1. Compute e=H(M) (e is an integer)
2. Generate a random integer k
3. Compute R=kP=(x,y)
4. Convert x to an integer.
5. Compute r=x+e mod n
6. Compute s=k−ar mod n.
7. The signature is (r,s).

Since R=kp is computed independently of the message M it could be pre-computed prior to signing M which occurs in steps (5) and (6). In this procedure, the time to hash and generate a random number is taken to be negligible in comparison with other operations performed. Finally, pre-computation of certain functions may be performed to speed up the computation of kP in step (3).

Any entity B can verify A's signature (r,s) on M by performing the following steps:

1. Obtain A's public key Y_a=aP.
2. Compute u=sP
3. Compute V=rYa
4. Compute u+v=(x',y')
5. Convert x' to an integer.
6. Compute e'=r−x' mod n.
7. Compute e=H(M) and verify that e'=e.

The following example illustrates encryption using an elliptic curve encryption scheme. Assume that Entity A has a private key a and public key Ya=aP where P is a generating point. Entity B encrypts bit string M to entity A using the following procedure:

1. B obtains A's public key Y_a
2. B generates random integer k.
3. B computes R=kP.
4. B computes $S=kY_a=(x,y)$
5. B computes $c_i=m_i \approx f_i(x)$.
6. B sends $(R,c_o \ldots c_n)$ to A.

Where $f_0(x)$=SHA-1(x‖0) and $f_i(x)$=SHA-1($f_{i-1}(x)$‖x‖i)

Alternatively, if RSA cryptography is used, the following definitions are pertinent:

n is the modulus.

d is the private key and the public exponent for entity A.

M is a bit string to be signed.

An RSA signature is generated by Entity A as follows:

1. Compute m=H(M), an integer less than n.
2. Compute $s=m^d \bmod n$
3. The signature is s.

RSA signing as described above creates digital signatures with appendix. In contrast to the ECC signing discussed previously, no pre-computation is possible when using RSA. Note that the signing requires one exponentation by the private exponent d.

Entity B can verify A's signature S on M using the following procedure:

1. Obtain A's public exponent e and modulus n.
2. Compute $m^*=s^e \bmod n$.
3. Compute m=H(M).
4. Verify that $m^*=m$

In RSA verification, one exponentation by the public exponent e is required. e is preferably selected to be 64 random bits. Similarly, for RSA encryption, one exponentation is required with a public exponent and the public exponent should be at least 64 bits long for minimum security.

In view of the preceding discussion, the remainder of the secure messaging system is described with reference to FIGS. **10–16**. One of ordinary skill in the art will readily discern that the system discussed herein may be modified to take best advantage of the disclosed or similar cryptographic schemes to insure complete integrity of the secure financial transaction.

Referring to FIG. **10**, the illustration shows a high level block diagram of a financial messaging unit **906** in accordance with the preferred embodiment of the present invention.

One possible embodiment of a financial messaging unit **906** is a conventional paging device and Smart Card **920** combination as shown in FIG. **10**. Here, a mechanical slot and standard Smart Card connector **1042** are incorporated into the paging device's housing so that a Smart Card **920** can be inserted into the housing in a manner that establishes electrical contact between the card and the financial messaging unit's **906** electronics. Alternatively, the electronics required to implement a Smart Card **920** are moved or integrated into the financial messaging unit **906**so the financial messaging unit **906** functions as a true wireless Smart Card or wireless ATM.

Operationally, the incoming signal is captured by the antenna **802** coupled to the receiver **804** which detects and demodulates the signal, recovering any information as previously discussed with reference to FIG. **8**. Alternatively, the financial messaging unit **906** contains a low power reverse channel transmitter **1034**, power switch **1032**, and transmit antenna **1030** for either responding to an outbound channel query or generating an inbound channel request. Instead of the portable transmitter **1034** (e.g., a low power radio frequency device) and its associated components, the alternative transmission block **1036** may contain either uni- or bi-directional communication transducers, or preferably in a 1-way device, a message origination unit **138** comprising a transducer **1040** is coupled to the processor **1006** in the secure financial messaging unit **906**. Examples of suitable transducers are optical devices like lasers or light emitting diodes (LED), extremely low power magnetic field inductive or electric field capacitive structures (e.g., coils, transmission lines or the like), and possibly acoustic transducers in the audio or ultrasonic range.

An input/output (I/O) switch **1002** serves to direct the incoming or outgoing radio frequency (RF) energy between the RF receiver **804**, RF transmitter **1030** and a selective call decoder **1004**. The selective call decoder **1004** comprises a processing unit **1006**, and its associated random access memory (RAM) **1008**, read-only memory (ROM) **1010**, and universal input/output (I/O) module **1012**. The primary function of the selective call decoder **1004** is to detect and decode information contained in signalling intended for receipt by the financial messaging unit **906**. Alternatively, in a 2-way implementation that includes the optional reverse channel transmitter block **1036** and/or the message origination unit **1038**, the selective call decoder **1004** may also function as an encoder to generate and deliver requests or messages to the regulator **914**, a user, or other on-line system (not shown).

Additionally, the financial messaging unit **906** comprises a secure decoding or Smart Card function module **1014** that serves as a second financial transaction processor. This module comprises control logic **1016**, a message entry device **1018**, a security code processor **1020**, a secure ROM **1022**, a secure programmable read only memory (PROM) **1024**, and a Smart Card input/output (I/O) module **1026**.

Certain financial groups have proposed standards for effecting end-to-end transaction security in the land-line wired environment. The standards proposed for securing electronic financial transactions are based on a peer-to-peer closed loop system in which the sending party (e.g., a regulator or issuer such as a bank, or VISA™) generates a secure transaction that comprises a value amount and an authentication code. The secure transaction is communicated **924** to a requesting party via a device such as an ATM **926**. In order to establish and complete a transaction, the requesting party inserts a Smart Card **920** into the ATM, enters an identification code, and requests a value to be placed in the Smart Card **920**. The transaction processing system authenticates the Smart Card **920**, the requesting party's financial status (e.g., account balance, credit availability, etc.) and either completes or denies the transaction.

Accordingly, in view of the above requirements, the control logic **1016** operates to govern operation of the components associated with the Smart Card function module **1014** to implement and maintain end-to-end security in a secure financial transaction message. The control logic **1016** insures that any contents associated with the secure financial transaction message are kept in their encrypted state from a regulator **914** until they are actually decrypted by the Smart Card function module **1014** or an associated Smart Card **920**. Therefore, sensitive information such as a private encryption key, cash load values, credit or bank account numbers, or the like, are stored in the secure PROM **1024**. Similarly, the secure ROM **1022** may store processing routines that decrypt and encrypt information exchanged between the Smart Card function module **1014** and a regulator **914**, merchant **916**, or another Smart Card **920**.

The message entry device **1018** allows a user to initiate a cash load request, cash transaction, credit transaction, or the like. Typically, a user might enter a request using a keyboard, a voice activated recognition device, a touch-sensitive device (erg., screen or pad), or other convenient data entry device. In the present invention, a user may request transaction based information be communicated with the financial messaging unit **906**, stored in the financial messaging unit **906** for later transfer to the Smart Card **920**, or passed directly to the Smart Card **920**. In this way, the financial messaging unit **906** acts like a portable ATM, allowing a user to effect financial transactions without actually visiting a physical ATM.

In the case where the financial messaging unit **906** acts like a portable ATM with origination capability, the Smart Card function module **1014** operates as a second secure message generator coupled to the financial messaging unit to create a financial transaction request. Once created, a portable transmitter **1034** coupled to the secure message generator operates to broadcast the financial transaction request to a selective call message processor **1104**. A receiver **1204** coupled to the selective call message processor **1104**operates to receive and couple the financial transaction request to the selective call message processor **1104**. In this way, the financial messaging unit **906** can perform financial transactions without requiring a physical connection to a land-line hard wired network or PSTN.

With regard to the implementation of a radio frequency enabled reverse channel financial messaging unit **906** as discussed herein, the invention preferably operates using the Motorola ReFLEX™ 2-way wireless paging system infrastructure and protocol which is described in detail in the following documents:

It should be appreciated that the use of the instant invention in other 2-way communication systems such as cellular and radio packet data systems is contemplated.

Certain financial groups have proposed standards for effecting end-to-end transaction security in the land-line wired environment. The standards proposed for securing electronic financial transactions are based on a peer-to-peer closed loop system in which the sending party (e.g., a regulator or issuer such as a bank, or VISA™) generates a secure transaction that comprises a value amount and an authentication code. The secure transaction is communicated to a requesting party via a device such as an Automatic Teller Machine (ATM). In order to establish an complete a transaction, the requesting party inserts a Smart Card **920** into the ATM, enters an identification code, and requests a value to be placed in the Smart Card **920**. The transaction processing system authenticates the Smart Card **920**, the requesting party's financial status (e.g., account balance credit availability, etc.) and either completes or denies the transaction.

In a broader application, the financial messaging unit **906** may be adapted to communicate, sensitive messages or data, as well as electronic funds transfer information can be securely transferred to the intended recipient device via a paging channel or the like.

Referring to FIG. **11**, the block diagram illustrates message composition and encryption equipment that could be used on the premises of a financial institution to send secure electronic funds transfer authorizations to financial messaging units via a paging channel or the like.

Specifically, both direct branch and customer calls are received by a first financial transaction processor **1100** comprising a transaction processing computer **1102**, a message processing and encryption computer **1104** or selective call message processor that operates as a first secure message generator, a first secure message decoder, and a selective call message distributor, all being functions of the selective call message processor **1104**, a subscriber database **1106**, and a security code database **1108**. The transaction processing computer **1102** receives financial transaction requests and communicates with the message and encryption processor **1104** to generate and encrypt secure financial transaction message based on information contained in the security code database **1108** corresponding with the requester and the transaction type. The message processing and encryption computer **1104** also determines a destination identifier from information contained in the subscriber database **1106**, which allows the selective call message distributor to communicate the destination identifier and its corresponding secure financial transaction message to a selective call transmission service **904**. The destination identifier may correspond with a conventional paging address, a cellular telephone address, or any other address that uniquely identifies a destination associated with the secure financial transaction message.

The message composition and encryption equipment illustrated in FIG. **11** would typically be used on the premises of a financial institution to send secure electronic funds transfer authorizations to financial messaging units **906** (e.g., "wireless ATM" devices) via a conventional paging channel or the like. In the following examples, the transaction information is composed using standard financial computers and data structures, and the message is encrypted using the public and private keys assigned to target device and transaction, respectively. The keys assigned to each device, along with their paging addresses, are stored in the user database associated with the processing computer. After each message is encrypted, it is sent like a normal paging message to the paging system via the public telephone system.

The first financial transaction processor **1100** will be more fully discussed with reference to FIG. **12** which integrates the first financial transaction processor **1100** with a wireless selective call signaling system controller.

Referring to FIG. **12**, the illustration shows a functional diagram of a wireless selective call signaling system controller that implements a combined 1-way and 2-way secure messaging system capable of signalling the financial messaging units.

The wireless selective call signaling system controller **1200** comprises the first financial transaction processor **1100** along with a transmitter **104** and associated antenna **904**, and in 2-way RF systems, at least one receiver **1202** system comprising a received signal processor **1204** and at least one receive antenna **908**. Preferably, several of at least one receiver **1202** systems may be distributed over a wide geographical area to receive the low power transmissions broadcast by 2-way financial messaging units **906**. The number of receiver **1202** systems in any given geographical area is selected to insure adequate coverage for all inbound transmissions. As one of ordinary skill in the art will appreciate, this number may vary greatly depending on terrain, buildings, foliage, and other environmental factors.

The wireless selective call signaling system controller **1200** represents a closely coupled implementation of the overall secure messaging system. In practice, a regulator (e.g., bank, credit card issuer, etc.) may not want the responsibility of maintaining the RF infrastructure, i.e., the transmitter **104** and associated antenna **904**, and the at least one receiver **1202** system. Consequently, a conventional wireless messaging service provider or the like would provide and maintain the RF infrastructure, and the regulator would utilize that RF infrastructure in a conventional manner to communicate secure financial transaction messages between the regulator and the financial messaging units **906**.

As a first alternative to the preceding operation, the selective call signaling system controller **1200** may operate to encrypt, encode, and transmit secure financial transaction messages received from a regulator, where the first financial transaction processor **1100** has generated and encrypted the secure financial transaction message, and the selective call signaling system controller **1200** further encrypts the secure financial transaction message, for a second time. This increases the level of security of an associated secure

financial transaction message by encapsulating it using a second, unrelated encryption. Subsequently, the financial messaging unit **906** decodes and decrypts the doubly encrypted message, revealing the secure financial transaction message in its encrypted state, and thus maintaining the end-to-end security required for a financial transaction. Similarly, the selective call signaling system controller **1200** receives messages originating from the financial messaging unit **906** and passes the secure financial transaction message in its encrypted state to a regulator for decryption and processing.

As a second alternative to the preceding operation, the selective call signaling system controller **1200** may operate to encode and transmit secure financial transaction messages communicated between the regulator and the financial messaging unit **906**. In this case, the first financial transaction processor **1100** at the regulator has generated and encrypted the secure financial transaction message, and the selective call signaling system controller **1200** operates to associate a selective call address with the secure financial transaction message based on a received destination identifier, then transmit a resulting selective call message for receipt by the financial messaging unit **906**. Subsequently, the financial messaging unit **906** decodes the selective call message, revealing the secure financial transaction message in its encrypted state, and thus maintaining the end-to-end security required for a financial transaction. As with the prior operation, the selective call signaling system controller **1200** further operates to receive messages originating from the financial messaging unit **906** and passes the secure financial transaction message in its encrypted state to a regulator for decryption and processing.

Referring to FIG. **13**, the illustration shows the various layers of a messaging system in a format that is similar to the Organization Standards International (OSI) stack diagram that is well known in the electronics industry.

With respect to the present invention, the network layer **1302** is a point at which financial transactions are created. These financial transactions are then communicated to a messaging layer **1304** where appropriate selective call messages are formed for inclusion in a transport protocol such as Motorola's FLEX or POCSAG. The channel signalling layer **1306** or transport layer represents the point where the low level transport protocols mentioned above are implemented. Finally, the RF channel **1308** is the physical media on which the low level transport protocol communicates the selective call messages containing the financial transactions.

Referring to FIG. **14**, the flow diagram shows typical operation of a financial messaging unit in accordance with the preferred embodiment of the present invention.

When activated **1400**, the financial messaging unit **906** (denoted as a pager for clarity of explanation) operates "normally," that is, it waits in a standby state **1402** searching for its selective call address **1404**. If the financial messaging unit detects its address, and in particular it detects a security address **1406**, e.g., a specific selective call address associated with a single unique account, or one of several unique accounts, the financial messaging unit **906** recovers the secure financial transaction message to effect a financial transaction. If steps **1404** or **1406** fail, control returns to step **1402** in which the financial message unit resumes normal operation. Once the financial messaging unit **906** determines that a secure financial transaction message is received, the Smart Card function module **1014** is activated **1408** and the secure financial transaction message may be decoded **1410**. Decoding as mentioned here can represent the recovery of the secure financial transaction message from the native selective call protocol, e.g., from a FLEX™ or POCSAG data or information word, or decoding can include the step of decrypting the secure financial transaction message to recover its contents representing an electronic cash token value, a credit value, a debit value, or other information relating to a secure financial transaction such as cryptographic message or session keys. According to the content of the secure financial transaction message, the control logic **1016** and processor **1006** operate to execute instructions **1412** pertinent to the financial transaction being executed.

Referring to FIG. **15**, the illustration shows a typical sequence associated with requesting and authorizing the electronic transfer of funds or debit of funds by and from a wireless financial messaging unit.

A financial transfer sequence is initiated **1500** by a customer calling his or her bank **1502**, identifying themselves **1504** via a PIN number or other account information **1506**, and requesting a transfer or other financial transaction **1508** for communication to their wireless financial messaging unit **906**.

After verifying the identity of the customer **1510** and the appropriate account information **1512**, the bank or regulator initiates a sequence of events to effect the electronic transfer of the funds, granting of credit, or the like **1604**. In a first case, a financial transaction is approved when the financial transaction request is authenticated as originating from an authorized party and the financial transaction is permitted by a regulator **1514**. Typically, regulators permit financial transactions when a party has sufficient funds as in a cash load or debit request, or when a party has sufficient credit available to complete a transaction. Preferably, upon approval, the financial messaging unit **906** prompts the user to wait for the transaction **1520** and the system begins completion of the financial transaction **1522**.

In a second case, the first financial transaction processor denies completion of the financial transaction based on the financial transaction request when at least one of the financial transaction request is not authenticated as originating from an authorized party and the financial transaction is not permitted by a regulator **1516**. Typically, regulators deny financial transactions when a party has insufficient funds in the cash load or debit request, or when a party has insufficient credit available to complete a transaction. If the regulator denies the financial transaction, the request is terminated **1518** and the financial messaging unit **906** returns to normal operation.

Referring to FIG. **16**, the illustration shows a typical sequence associated with the wireless transfer of funds or debit of funds by and from a wireless financial messaging unit in both a 1-way and a 2-way secure communication system.

Completion of the financial transaction **1522** begins by the regulator or issuer looking up the destination identifier and security code (e.g., public or private key) for a user account **1602** associated with at least one financial messaging unit **906**. The secure messaging system then generates the secure financial transaction message which is communicated to the wireless selective call signaling system controller where the selective call message processor **1104** executes a control program that receives selective call message requests comprising a destination identifier and the secure financial transaction message and encapsulates the secure financial transaction message in a selective call message that includes a selective call address corresponding with the destination identifier. This selective call message is then distributed to a selective call transmission service in response to the destination identifier. The selective call

transmission service broadcasts the selective call message to the financial messaging unit **906** that receives the selective call message. Optionally, the financial messaging unit **906** may send a first message prompting the user to insert a Smart Card **920** for funds transfer or the like. The bank would then wait **1606** an appropriate time period **1608**, then send a data transmission comprising information with the account number of the Smart Card **920** to be credited, the amount of the transaction, and coded information to verify that the Smart Card **920** to be debited is valid and not a counterfeit **1610**. Obviously, if the Smart Card **920** is integrated with the financial messaging unit **906**, steps **1604**, **1606**, and **1608** need not be performed. A bank will typically record **1612** the success or failure of a transaction upon its completion **1614**.

In a financial messaging unit **906** having 2-way capability **1616**, the bank can wait for receipt of an acknowledgment **1618** comprising a returned secure financial transaction message that confirms execution of the financial transaction. When the financial transaction is successfully completed, an optional message may be presented **1624** to the user at the financial messaging unit **906** before the financial messaging unit **906** returns to an idle state **1626**. Alternatively, if no acknowledgment is received after a predetermined delay period **1620**, the bank may re-initiate the prior financial transaction **1622**.

In a variation of the operation discussed in reference to FIGS. **14–16**, the user may remain in communication during the financial transaction, and the bank may receive a non-real time acknowledgment that the transaction was completed successfully using an alternate path, i.e., one other than the RF reverse channel. This can be accomplished by either using a 1-way or 2-way paging device in a wired ATM machine, or by having the user remain on a phone or other communication device during the entire transaction. Additionally, a distinctive audio alert pattern can be generated by the financial messaging unit **906** to signal that the financial transaction has been completed without error.

Additionally, if an address is detected that is associated with a normal messaging function, the financial messaging unit **906** will operate as a normal paging device. However, if the detected address is associated with a secure data transmission address, the secure decoder module may be activated, the received secure financial message may be decrypted, and the information contained in the message would be processed in accordance with either the contents of the message or with the rules associated with the received address.

Referring to FIG. **17**, the flow diagram depicts a typical sequence associated with either authentication or confirmation of a wireless transfer of funds, debit of funds, or credit transaction between a wireless financial messaging unit and a regulator in either a 1-way or a 2-way secure communication system.

In order to maintain confidentiality of the financial information being exchanged between a host (e.g., an issuer, regulator, merchant or the like) and the financial messaging unit, all transactions transmitted or received (communicated) between the secure financial messaging unit and the host, wireless communication or paging system, ATM, and point of sale terminal should be encrypted. The Secure Electronic Transaction protocol (SET) developed by several major financial entities defines the use of cryptographic techniques along with a rule set for effecting secure electronic financial transactions in a wire-line environment. The SET protocol may be easily adapted to accommodate both 1-way and 2-way wireless financial transactions using the secure financial messaging unit. Specifically, SET requires that in most cases a Smart Card **920** device or other device operating as a Smart Card (e.g., an enabled secure financial messaging unit **906**) communicate bi-directionally with a regulator to effect a financial transaction Consequently, an conventional 1-way wireless communication device like a pager cannot an will not be accepted or approved for use as a wireless financial messaging unit. However, using the features discussed in reference to the instant invention, a conventional 1-way paging device, or any other device (e.g., an electronic wallet) capable of being adapted for operation like a conventional 1-way paging device, can be modified to include a local or wide area communication capability required to "close the loop" with the regulator.

To further accommodate such financial messaging units **906**, the SET protocol is preferably extended to allow non-real time confirmation and authentication of financial transactions. Since typical SET confirmation and authentication messages are much too long to enter manually using a DTMF keypad or the like (several hundred keystrokes would be required), the transducer **1040** in the message origination unit **1038** is used to generate reverse channel communications under control of the processor **1006** and the Smart Card function module **1014**. For example, if an acoustic audio transducer is selected it might be used to generate DTMF dialing codes, then send the encrypted communication of the confirmation response via the PSTN **912** using International Telecommunication Union (ITU) modem standards, e.g., V.22, V.32, V.34, or the like.

Currently, a SET transaction is secure not only because of its encrypted state, but because of a finite time associated with a financial session established to effect the financial transaction. This time window during which the financial transaction must be completed can be modified in instances where a financial transaction such as a fund transfer (cash load) between a bank and a financial messaging unit **906**, between two financial messaging units **906**, or possibly between a Smart Card **920** at a first location and a financial messaging units **906** or Smart Card **920** in a second location inserted in a financial messaging unit **906** is requested.

According to the present invention, a conventional selective call message is broadcast to a selected financial messaging unit **906**, the conventional selective call message containing a secure financial transaction. The selected financial messaging unit **906** receives and decodes the conventional selective call message, then presents a user with a notification that a financial transaction is in progress, optionally indicating an action required and possibly the type of transaction being effected. For example, if a business traveler needed more money during an extended business trip, conventional wisdom dictates that he would visit a bank or other source of cash. However, with a financial messaging unit **906**, the business traveler could request more funds by calling a prearranged number, entering their identification code, and requesting an amount to be sent to their financial messaging unit **906**. Alternatively, if the business traveler is near an ATM or point of sale terminal, they can initiate a funds request from the financial messaging unit **906** using any number of input devices such as a touch sensitive input pad, keyboard, voice recognition device, or the like. In that case, the financial messaging unit **906** generates a message and contacts a regulator **914** using a local link **924** between the message origination unit and at least one of a point of sale terminal **928** and an ATM **926**. The regulator **914** then generates the secure financial transaction message that is encapsulated in a standard selective call signalling protocol

message and broadcast to the requesting financial messaging unit **906**. The requesting financial messaging unit **906** receives the selective call message including a response to the message in the form of the secure financial transaction message **1702**. Preferably, the selective call message is broadcast from a wide area selective call signalling system so wherever the requesting financial messaging unit **906** is located, it will receive the selective call message. After decoding the selective call message to recover the secure financial transaction message, the requesting financial messaging unit **906** decrypts a content of the secure financial transaction message to reveal instructions representing the actual financial transaction. Several forms of the decrypted message are possible as defined in the latest SET specification, and may comprise the following: a session or message cryptographic key, a Diffie-Hellman key agreement/exchange component, a digital signature in a singular or impressed form, a certificate request, transaction instructions such as a unit identification request, a text or canned message that should be presented to the user **1704** of the requesting financial messaging unit **906** indicating that at least one of a confirmation and an authentication of the financial transaction associated with the secure financial transaction message is requested or designating a action required of the user such as entry of a personal identification number (PIN), authentication and confirmation codes, a transaction serial or tracking number, or tokens representing cash, debit, or credit values. One of ordinary skill in the art will readily discern that this list is only exemplary, and other components that become necessary based on the transaction type are possible.

Once the secure financial transaction message is decrypted, the financial messaging unit **906** selects **1706** at least one of the optical, electromagnetic, and acoustic transducers **1040** in the message origination unit **1038** to communicate a response to the secure financial transaction message. The financial messaging unit **906** then operates to contact **1710** the regulator **914** using a local link **924** between the message origination unit **1038** and at least one of the point of sale terminal **928** or ATM **926** to communicate the response to the secure financial transaction message. If the point of sale terminal **928** or ATM **926** is coupled via a land-line **910** to the PSTN **912**, either these devices or the message origination unit **1038** can dial a number **1708** representing the regulator **914**. The number may either be a predetermined number that is preferably stored in non-volatile secure ROM **1022** or EEPROM **1024** in the financial messaging unit **906**, or to increase security, a number that is received in a secure financial transaction message. If a dial-up response is required, the financial messaging unit **906** should not display the return telephone number received in the secure financial transaction message, but instead, should display a message such as "CONFIRMATION REQUIRED," thus prompting the user to obtain transaction confirmation to gain use of the credit or funds requested or funds transferred to the financial messaging unit **906**. Additionally, depending on the type of financial transaction being effected, the regulator **914** may request identification of the financial messaging unit **906**, a serial number of the current transaction, etc., as a confirmation message **1710** communicated either before of after completion of the financial transaction. Once the regulator determines that the financial messaging unit **906** is authentic and communications therefrom are confirmed and authenticated, the regulator broadcasts a message to the financial messaging unit **906** authorizing execution of the requested transaction. In this manner, a primarily 1-way wide area communication device such as the financial messaging unit **906**, and even a 2-way wide area communication device can securely conduct primarily wireless financial transactions.

One of ordinary skill in the art will appreciate that the preceding discussion regarding the claimed invention in not meant to limit the system to a particular transport protocol, wireless media, cryptographic scheme, or physical communication device. Consequently, the claimed invention and other variations made possible by the teachings herein represent only a few select ways that a secure messaging system for communicating financial information can be implemented using the unique principles taught in the present invention.

It is in the preceding spirit that we claim the following as our invention:

1. A secure financial messaging unit, comprising:

a wide area radio frequency receiver;

a selective call decoder coupled to the wide area radio frequency receiver;

a financial transaction processor coupled to the selective call decoder;

a main processor coupled to the financial transaction processor and the selective call decoder; and

a message origination unit coupled to the main processor, the message origination unit operating in at least one of a reply and confirmation mode and an originate and request mode to effect a wireless financial transaction using a local area link.

2. The secure financial messaging unit according to claim **1** wherein the message origination unit comprises:

a transducer coupled to the main processor, the transducer operating to couple a secure financial transaction message between the secure financial messaging unit and a regulator using the local area link to effect the wireless financial transaction.

3. The secure financial messaging unit according to claim **2** wherein the transducer comprises:

an optical device that communicates information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

4. The secure financial messaging unit according to claim **3** wherein the optical device comprises:

an light detector that detects light in a visible spectrum.

5. The secure financial messaging unit according to claim **3** wherein the optical device comprises:

an light detector that detects light in an infrared spectrum.

6. The secure financial messaging unit according to claim **3** wherein the optical device comprises:

an light detector that detects light in an ultraviolet spectrum.

7. The secure financial messaging unit according to claim **3** wherein the optical device comprises:

an light detector that detects light in any spectrum.

8. The secure financial messaging unit according to claim **3** wherein the optical device comprises:

an light emitting diode that emits light in a visible spectrum.

9. The secure financial messaging unit according to claim **3** wherein the optical device comprises:

an light emitting diode that emits light in an infrared spectrum.

10. The secure financial messaging unit according to claim 3 wherein the optical device comprises:

an light emitting diode that emits light in an ultraviolet spectrum.

11. The secure financial messaging unit according to claim 3 wherein the optical device comprises:

an light emitting diode that emits laser light in any spectrum.

12. The secure financial messaging unit according to claim 2 wherein the transducer comprises:

an acoustic device that communicates information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

13. The secure financial messaging unit according to claim 12 wherein the acoustic device comprises:

an audio transducer that detects audio energy in an ultrasonic spectrum.

14. The secure financial messaging unit according to claim 12 wherein the acoustic device comprises:

an audio transducer that detects audio energy in an audible spectrum.

15. The secure financial messaging unit according to claim 12 wherein the acoustic device comprises:

an audio transducer that emits audio energy in an ultrasonic spectrum.

16. The secure financial messaging unit according to claim 12 wherein the acoustic device comprises:

an audio transducer that emits audio energy in an audible spectrum.

17. The secure financial messaging unit according to claim 2 wherein the transducer comprises:

an electromagnetic device that communicates information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

18. The secure financial messaging unit according to claim 17 wherein the electromagnetic device comprises:

a magnetic field transducer that detects information broadcast from the local area link.

19. The secure financial messaging unit according to claim 17 wherein the electromagnetic device comprises:

an electric field transducer that detects information broadcast from the local area link.

20. The secure financial messaging unit according to claim 17 wherein the electromagnetic device comprises:

a magnetic field transducer that broadcasts information to the local area link.

21. The secure financial messaging unit according to claim 17 wherein the electromagnetic device comprises:

an electric field transducer that broadcasts information to the local area link.

22. The secure financial messaging unit according to claim 2 wherein the local area link comprises a conventional acoustic telephone that is acoustically coupled to an acoustic transducer in the secure financial messaging unit for communicating information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

23. The secure financial messaging unit according to claim 2 wherein the local area link comprises an infrared enabled point of sale terminal that is optically coupled to an optical transducer in the secure financial messaging unit for communicating information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

24. The secure financial messaging unit according to claim 2 wherein the local area link comprises an infrared enabled automatic teller machine that is optically coupled to an optical transducer in the secure financial messaging unit for communicating information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

25. The secure financial messaging unit according to claim 2 wherein the local area link comprises an low power radio frequency enabled point of sale terminal that is magnetically coupled to a magnetic transducer in the secure financial messaging unit for communicating information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

26. The secure financial messaging unit according to claim 2 wherein the local area link comprises an low power radio frequency enabled point of sale terminal that is electrically coupled to an electric transducer in the secure financial messaging unit for communicating information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

27. The secure financial messaging unit according to claim 2 wherein the local area link comprises an low power radio frequency enabled automatic teller machine that is magnetically coupled to a magnetic transducer in the secure financial messaging unit for communicating information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

28. The secure financial messaging unit according to claim 2 wherein the local area link comprises an low power radio frequency enabled automatic teller machine that is electrically coupled to an electric transducer in the secure financial messaging unit for communicating information comprising the secure financial transaction message in at least one of a uni-directional and a bi-directional way with the local area link for at least one of initiating the wireless financial transaction, authenticating the wireless financial transaction, and confirming completion of the wireless financial transaction.

29. In a secure financial messaging unit, a method comprising the steps of:

receiving a selective call message including a secure financial transaction message, the selective call message being broadcast from a wide area selective call signalling system;

decoding the selective call message to recover the secure financial transaction message;

decrypting the secure financial transaction message recovered from the selective call message; and

presenting a message indicating that at least one of a confirmation and an authentication of a financial transaction associated with the secure financial transaction message is requested.

30. The method according to claim 29 comprising the steps of:

selecting at least one of a optical, an electromagnetic, and an acoustic transducer in a message origination unit to communicate a response to the secure financial transaction message; and

contacting a regulator using a local link between the message origination unit and at least one of a point of sale terminal and an automatic teller machine to communicate the response to the secure financial transaction message, the regulator being an authority that requested the at least one of the confirmation and the authentication of the financial transaction associated with the secure financial transaction message.

31. The method according to claim 30 comprising the steps of:

receiving at least one of a transaction authorization and a transaction confirmation from the regulator via at least one of the wide area selective call signalling system and the local link, thereby allowing the secure financial messaging unit to complete the financial transaction associated with the secure financial transaction message.

32. The method according to claim 30 comprising the steps of:

identifying the financial transaction associated with the secure financial transaction message to the regulator before allowing the secure financial messaging unit to complete the financial transaction associated with the secure financial transaction message.

33. The method according to claim 30 comprising the steps of:

identifying the secure financial messaging unit to the regulator before allowing the secure financial messaging unit to complete the financial transaction associated with the secure financial transaction message.

34. The method according to claim 30 comprising the steps of:

identifying the secure financial messaging unit to the regulator after allowing the secure financial messaging unit to complete the financial transaction associated with the secure financial transaction message.

35. In a secure financial messaging unit, a method comprising the steps of:

generating a message requesting a financial transaction;

selecting at least one of a optical, an electromagnetic, and an acoustic transducer in a message origination unit to communicate the message requesting a financial transaction;

contacting a regulator using a local link between the message origination unit and at least one of a point of sale terminal and an automatic teller machine, the regulator being an authority that governs the financial transaction;

receiving a selective call message including a response to the message, the selective call message being broadcast from a wide area selective call signalling system;

decoding the selective call message to recover a secure financial transaction message;

decrypting the secure financial transaction message recovered from the selective call message; and

presenting a message indicating that at least one of a confirmation and an authentication of the financial transaction associated with the secure financial transaction message is requested.

36. The method according to claim 35 comprising the steps of:

receiving at least one of a transaction authorization and a transaction confirmation from the regulator via at least one of the wide area selective call signalling system and the local link, thereby allowing the secure financial messaging unit to complete the financial transaction.

37. The method according to claim 35 comprising the steps of:

identifying the financial transaction to the regulator before allowing the secure financial messaging unit to complete the financial transaction.

38. The method according to claim 35 comprising the steps of:

identifying the secure financial messaging unit to the regulator before allowing the secure financial messaging unit to complete the financial transaction.

39. The method according to claim 35 comprising the steps of:

identifying the secure financial messaging unit to the regulator after allowing the secure financial messaging unit to complete the financial transaction.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,105,006
DATED : August 15, 2000
INVENTOR(S) : Walter Lee Davis et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On title page, add the following assignee:

Assignee: Motorola, Inc., Schaumburg, Ill

Signed and Sealed this

Fifth Day of June, 2001

Attest:

Attesting Officer

Nicholas P. Godici

NICHOLAS P. GODICI

Acting Director of the United States Patent and Trademark Office

US005343529A

United States Patent [19]

Goldfine et al.

[11] Patent Number: 5,343,529

[45] Date of Patent: Aug. 30, 1994

[54] **TRANSACTION AUTHENTICATION USING A CENTRALLY GENERATED TRANSACTION IDENTIFIER**

[76] Inventors: **Milton Goldfine**, 201 Ootsima Way, Loudon, Tenn. 37774; **Marvin Perlman**, 11000 Dempsey Ave., Granada Hills, Calif. 91344; **Robert A. Montgomery**, 306 Chuniloti Cir., Loudon, Tenn. 37774-2607

[21] Appl. No.: **127,893**

[22] Filed: **Sep. 28, 1993**

[51] **Int. Cl.**[5] **H04L 9/00**

[52] **U.S. Cl.** **380/23**; 380/24; 380/25; 380/30; 380/49; 340/825.31; 340/825.34

[58] **Field of Search** 380/23-25, 380/4, 30, 49, 50; 235/379, 380; 340/825.31, 825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,376,279	3/1993	Perlman et al.	235/380
4,672,572	6/1987	Alsberg	380/23
4,691,355	9/1987	Wirstrom et al.	380/23
4,694,492	9/1987	Wirstrom et al.	380/23
4,720,860	1/1988	Weiss	380/23
4,723,284	2/1988	Munck et al.	380/25
4,885,778	12/1989	Weiss	380/23 X

Primary Examiner—Bernarr E. Gregory
Attorney, Agent, or Firm—Allen N. Friedman

[57] **ABSTRACT**

Each access attempt transmitted to an authentication agency causes the agency to produce a request identifier unique to that request. The request identifier is transmitted back to the authentication code generator of the user initiating the access attempt, and to an authentication code generator in the agency. The agency also retrieves a user identifier from a database and sends it to its authentication code generator. Both the user's authentication code generator and the agency's authentication code generator independently combine, through identical or complementary transformations, the user identifier and the request identifier to form a user authentication code and an agency authentication code. The two authentication codes are presented by a comparator, which issues a permit signal only if the comparison indicates a match between the two authentication codes. The permit signal is transmitted to a transaction control device to permit the transaction to proceed. Since the authentication code is unique to each transaction attempt, interception of an authentication code will not permit an unauthorized user to successfully initiate another transaction. As an additional security feature, the user of irreversible transformations in the authentication code generator would prevent decoding of an intercepted authentication code and would not allow an unauthorized user to derive the user identifier associated with the transaction. As required by a particular application, additional levels of security can be achieved by using encryption steps in combination with the irreversible transformations at selected points in the process.

37 Claims, 6 Drawing Sheets

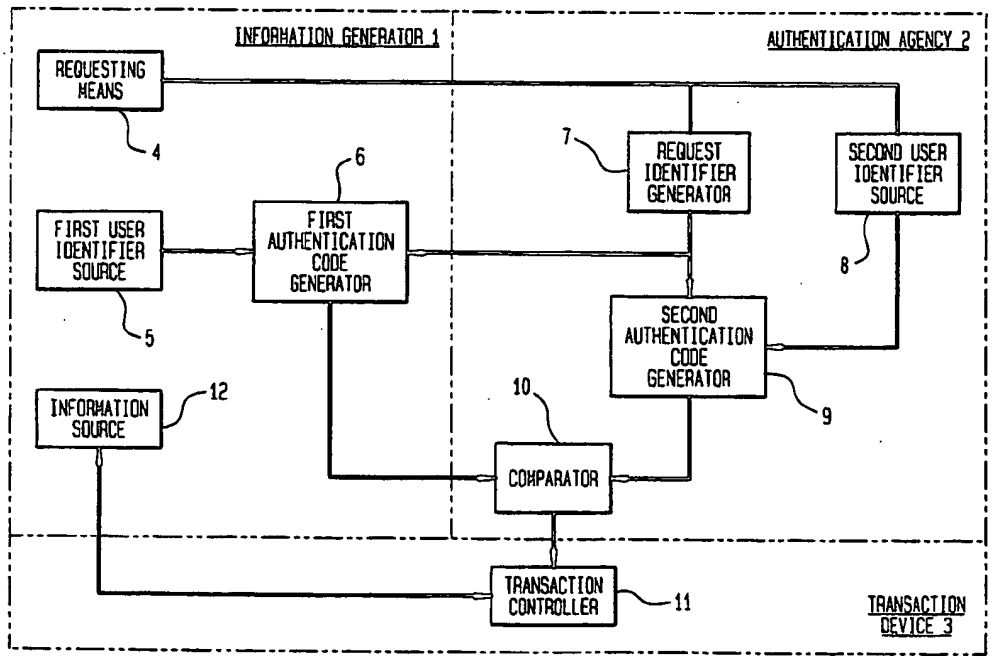


FIG. 1

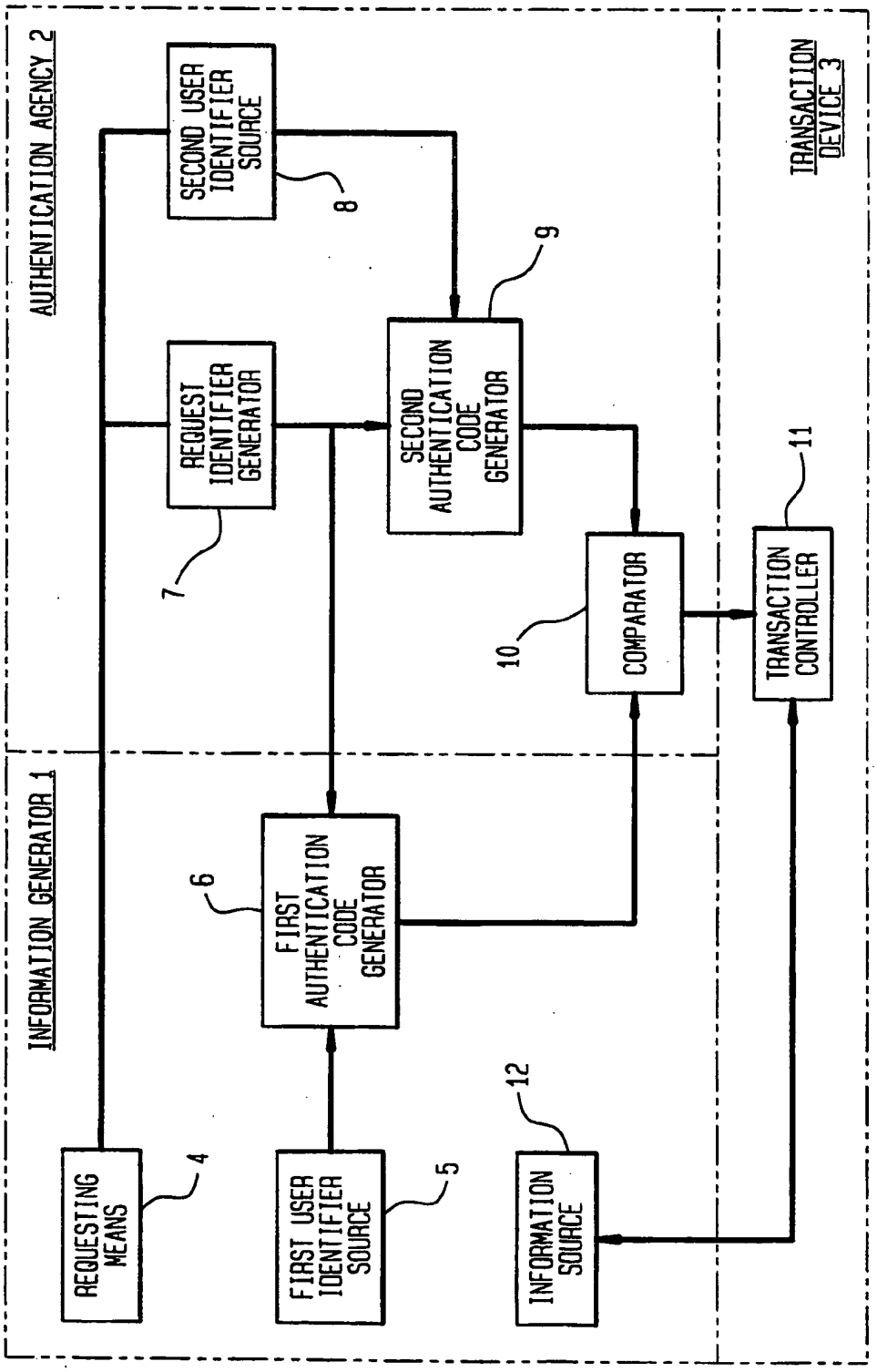

AUTHENTICATION AGENCY 2
TRANSACTION DEVICE 3
INFORMATION GENERATOR 1
SECOND USER IDENTIFIER SOURCE
8
9
REQUEST IDENTIFIER GENERATOR
7
SECOND AUTHENTICATION CODE GENERATOR
10
COMPARATOR
11
TRANSACTION CONTROLLER
6
FIRST AUTHENTICATION CODE GENERATOR
12
REQUESTING MEANS
4
FIRST USER IDENTIFIER SOURCE
5
INFORMATION SOURCE

FIG. 2

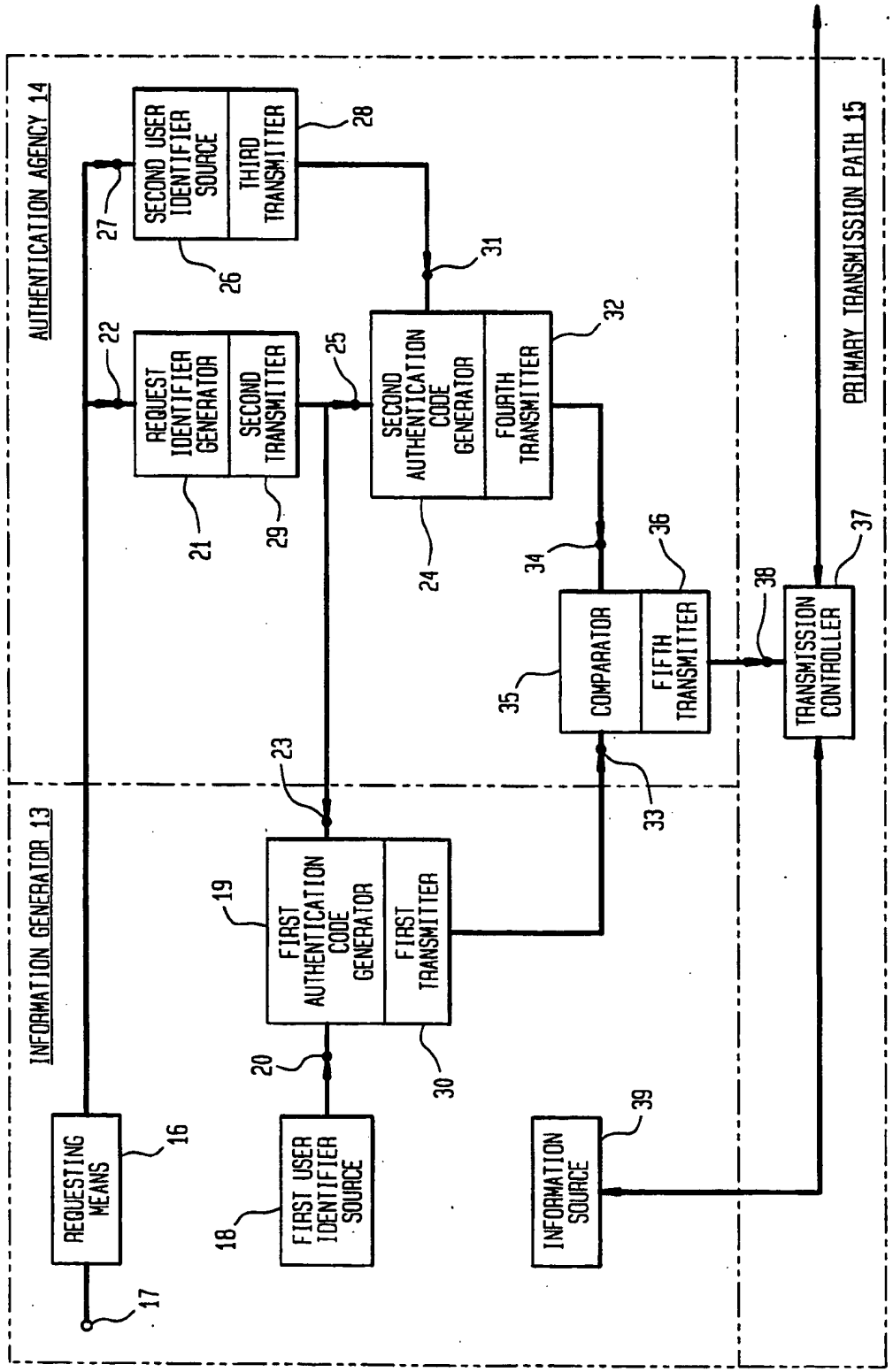
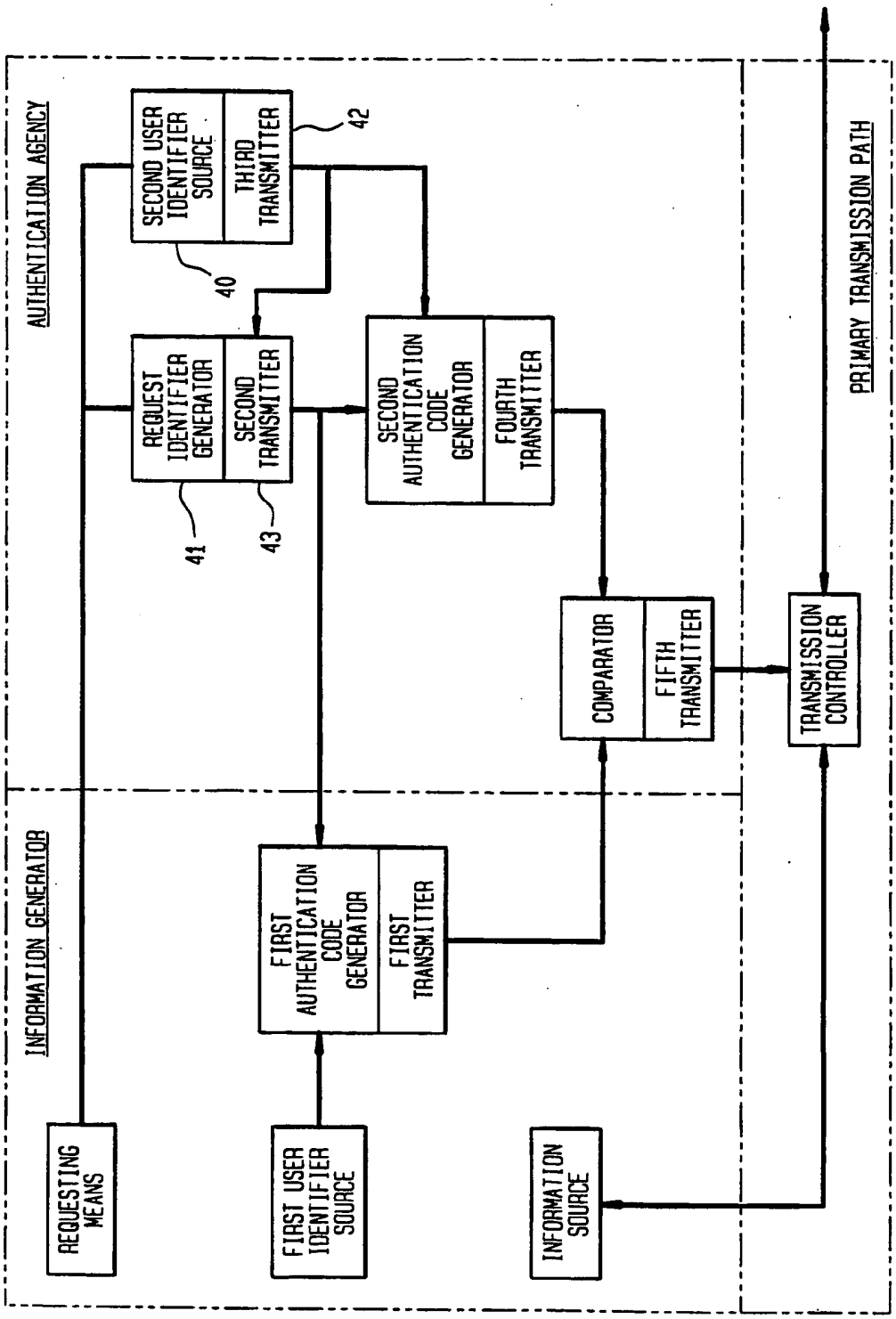

AUTHENTICATION AGENCY 14
INFORMATION GENERATOR 13
PRIMARY TRANSMISSION PATH 15
SECOND USER IDENTIFIER SOURCE
THIRD TRANSMITTER
REQUEST IDENTIFIER GENERATOR
SECOND TRANSMITTER
SECOND AUTHENTICATION CODE GENERATOR
FOURTH TRANSMITTER
COMPARATOR
FIFTH TRANSMITTER
TRANSMISSION CONTROLLER
FIRST AUTHENTICATION CODE GENERATOR
FIRST TRANSMITTER
REQUESTING MEANS
FIRST USER IDENTIFIER SOURCE
INFORMATION SOURCE
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

FIG. 3


AUTHENTICATION AGENCY
INFORMATION GENERATOR
PRIMARY TRANSMISSION PATH
SECOND USER IDENTIFIER SOURCE
THIRD TRANSMITTER
42
40
REQUEST IDENTIFIER GENERATOR
SECOND TRANSMITTER
41
43
SECOND AUTHENTICATION CODE GENERATOR
FOURTH TRANSMITTER
COMPARATOR
FIFTH TRANSMITTER
TRANSMISSION CONTROLLER
FIRST AUTHENTICATION CODE GENERATOR
FIRST TRANSMITTER
REQUESTING MEANS
FIRST USER IDENTIFIER SOURCE
INFORMATION SOURCE

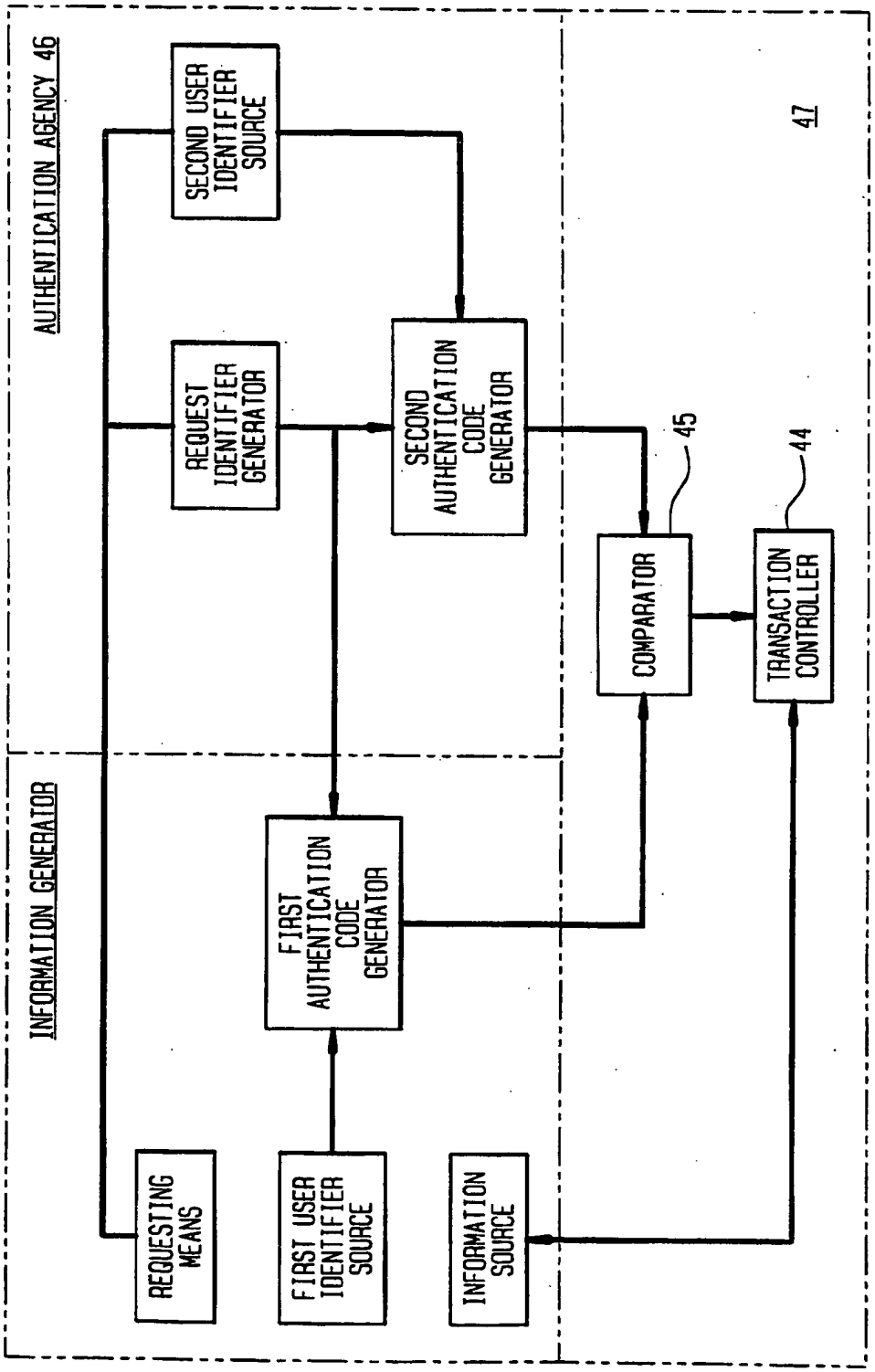

AUTHENTICATION AGENCY 46
SECOND USER IDENTIFIER SOURCE
REQUEST IDENTIFIER GENERATOR
SECOND AUTHENTICATION CODE GENERATOR
COMPARATOR
TRANSACTION CONTROLLER
45
44
47
INFORMATION GENERATOR
FIRST AUTHENTICATION CODE GENERATOR
REQUESTING MEANS
FIRST USER IDENTIFIER SOURCE
INFORMATION SOURCE

FIG. 4

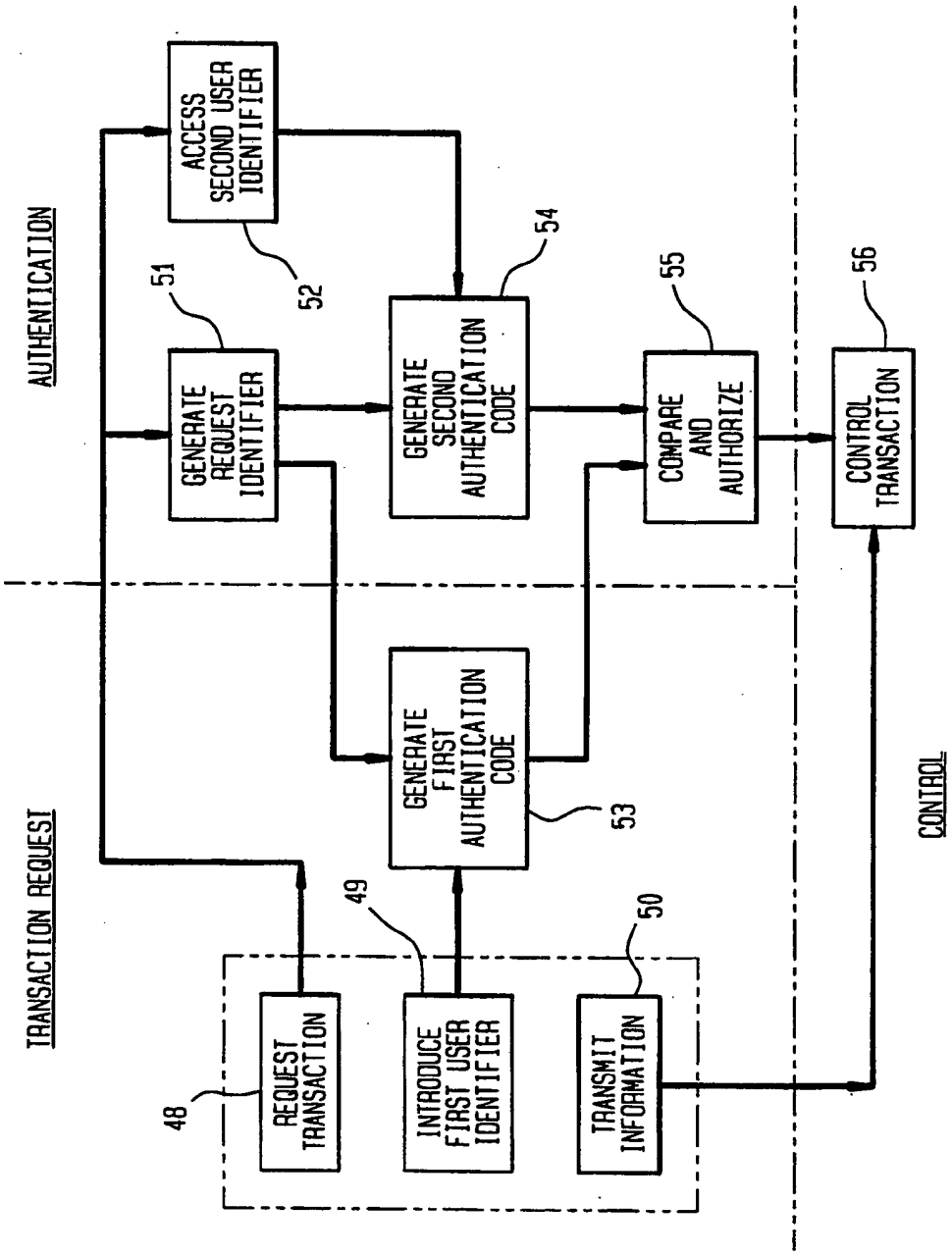
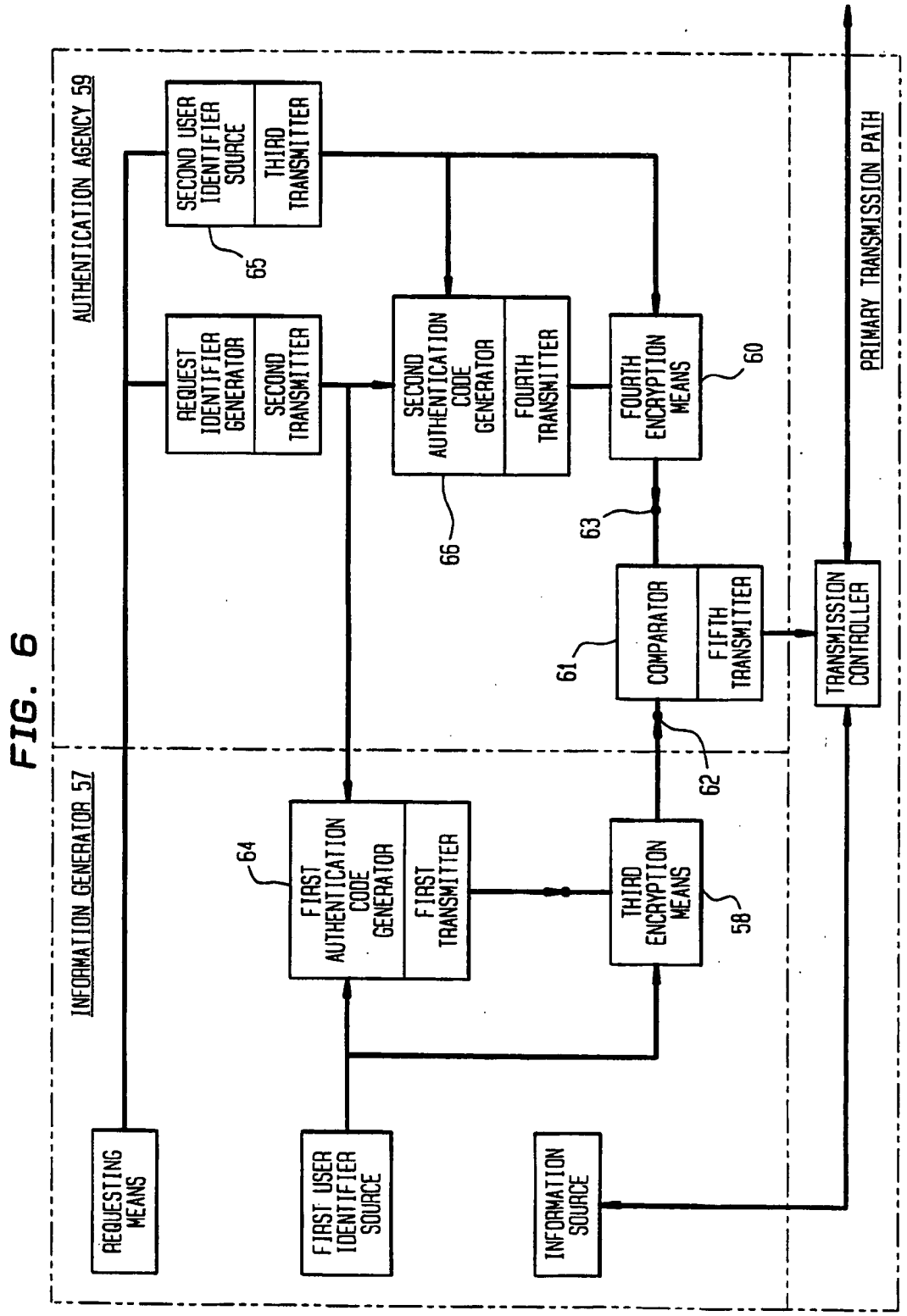

AUTHENTICATION
TRANSACTION REQUEST
CONTROL
ACCESS SECOND USER IDENTIFIER
GENERATE REQUEST IDENTIFIER
GENERATE SECOND AUTHENTICATION CODE
COMPARE AND AUTHORIZE
CONTROL TRANSACTION
GENERATE FIRST AUTHENTICATION CODE
REQUEST TRANSACTION
INTRODUCE FIRST USER IDENTIFIER
TRANSMIT INFORMATION
48
49
50
51
52
53
54
55
56

FIG. 5

FIG. 6


AUTHENTICATION AGENCY 59
INFORMATION GENERATOR 57
PRIMARY TRANSMISSION PATH
SECOND USER IDENTIFIER SOURCE
THIRD TRANSMITTER
65
REQUEST IDENTIFIER GENERATOR
SECOND TRANSMITTER
SECOND AUTHENTICATION CODE GENERATOR
FOURTH TRANSMITTER
66
FOURTH ENCRYPTION MEANS
60
63
COMPARATOR
FIFTH TRANSMITTER
61
62
TRANSMISSION CONTROLLER
64
FIRST AUTHENTICATION CODE GENERATOR
FIRST TRANSMITTER
THIRD ENCRYPTION MEANS
58
REQUESTING MEANS
FIRST USER IDENTIFIER SOURCE
INFORMATION SOURCE

TRANSACTION AUTHENTICATION USING A CENTRALLY GENERATED TRANSACTION IDENTIFIER

BACKGROUND OF THE INVENTION

1. Field of Invention

This invention authenticates a transaction request in order to permit progress of a transaction based on a match between an authentication code generated by the requestor of the transaction and an authentication code generated by an authentication agency.

2. Brief Description of the Prior Art

Central authentication of remote transactions is an important mode of business conduct. Remote access to electronic funds transfer networks must be authenticated to prevent theft of funds. Access to communications systems, such as cellular mobile radio systems, must be authenticated to prevent theft of communication services. Authentication is also important in governing electronic access to computer networks and interactive television and physical access to secured locations. Operators of these kinds of systems have developed a number of different techniques for reducing the susceptibility of their systems to various forms of fraud. However, almost all of these techniques can be circumvented by sophisticated misusers with enough computer resources at their disposal or by dishonest employees who can access the systems at various exposed points to steal access code information.

Many of the authentication techniques use combinations of passwords and personal identification numbers (PINs) to attempt to verify that the user attempting to access a network or service is authorized for access. Unauthorized access using PINs and passwords improperly obtained can be somewhat reduced by requiring users to periodically change these codes. A personal identification system disclosed in U.S. Pat. No. 4,376,279 uses a PIN secretly selected by the user, a code number secretly selected by officers of the authenticating agency and an irreversible transform secretly selected by the manufacturer of the system to produce a code number that is magnetically encoded onto a user card, such as a credit card or banking access card. Since only the user knows the selected PIN, the user's entry of that PIN, after inserting the card into the system presumably establishes that authority of that user to access the system. However, even though the system is partitioned to protect different portions of the access code information, changing access codes is cumbersome, so that the same information is used over and over again. An eavesdropper or other person that can obtain access to the transaction data and with enough computer power may, over time, accumulate enough information to learn the access code and gain unauthorized entry.

Theft of telecommunication services through eavesdropping on cellular mobile radio calls has become a major problem. The eavesdropper captures or derives the caller's access code, builds it into his radio unit, and makes subsequent unauthorized calls billed to the original caller. A long period of time could go by before this misuse is discovered and the access code changed. Hackers seeking access to telecommunication and computer networks program their computers to try thousands of access codes in an attempt to find one that works. Once a successful code is found, the hacker can gain network access. Similar problems will exist for emerging interactive television services, such as entertainment and home shopping. Authentication techniques that use repeatedly transmitted access codes are susceptible to various sophisticated attacks. Some technique is needed to keep the attackers off balance.

SUMMARY OF THE INVENTION

The transaction authentication method that is the subject of the present invention uses a centrally generated identifier that is specific to each transaction request to assure that the access information being transmitted from point to point in the system is different for each transaction attempt. In this transaction authorization process and apparatus, each access attempt transmitted to an authentication agency causes the agency to produce a request identifier unique to that request. The request identifier is transmitted back to the authentication code generator of the user initiating the access attempt, and to an authentication code generator in the agency. The agency also retrieves a user identifier from a database and sends it to its authentication code generator. Both the user's authentication code generator and the agency's authentication code generator independently combine, through identical or complementary transformations, the user identifier and the request identifier to form a user authentication code and an agency authentication code. The two authentication codes are presented to a comparator, which issues a permit signal only if the comparison indicates a match between the two authentication codes. The permit signal is transmitted to a transaction control device to permit the transaction to proceed. Since the authentication code is unique to each transaction attempt, interception of an authentication code will not permit an unauthorized user to successfully initiate another transaction. As an additional security feature, the use of an irreversible transformation in the authentication code generator would prevent decoding of an intercepted authentication code and would not allow an unauthorized user to derive the user identifier associated with the transaction. As required by the particular application, additional levels of security can be achieved by using encryption steps (reversible) in combination with the irreversible transformations at selected points in the process.

This invention produces a flexible transaction authentication architecture that can be used to meet the security needs of a diversity of transactions, such as authorizing a call to a remote access port of a telecommunication network or a cellular mobile radio call to access the network, allowing remote access to a computer network, identifying a user as an authorized electronic funds transfer agent or legitimate user of interactive television services, and permitting physical access to a secured location. Each of these transactions has different points of vulnerability to eavesdropping from the outside or compromise by dishonest insiders. The inventive architecture permits use of transformation and/or encryption of the authentication information at different points in the system dependent on an analysis of the particular application's vulnerabilities. In any event, the authentication information will be different for each transaction attempt, greatly impeding or entirely foiling efforts to successfully complete an unauthorized transaction.

With modern integrated circuit technology, the transformation involved can be economically realized in a microprocessor or special purpose VLSI chip. This

architecture gives the authorized user an economic advantage over the intended intruder. Since the authentication code changes in a virtually unpredictable way, an eavesdropper or intruder, collecting large amounts of data and applying much computer power, would find it practically impossible to determine a usable authentication code. However, the subject system compares authentication codes in their transformed or encrypted state without requiring inversion or decryption, which greatly simplifies the required equipment. The organization and operation of the invention can be better understood from consideration of the following detailed description of illustrative embodiments when read together with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 depicts a transaction authentication system of the invention.

FIG. 2 depicts a transaction authentication system of the invention in which the transaction is the transmission of information through a primary transmission path.

FIG. 3 depicts a system as depicted in FIG. 1 in which the second transmitter transforms the request identifier together with the second user identifier.

FIG. 4 depicts a system as depicted in FIG. 1 in which the comparator is associated with the transmission controller.

FIG. 5 depicts a transaction authentication method of the invention.

FIG. 6 depicts a system as depicted in FIG. 2 including means to encrypt the authentication codes.

DETAILED DESCRIPTION OF THE INVENTION

The following detailed description and several exemplary embodiments will help convey an understanding of the claimed invention. The invention is a method and apparatus embodying a system architecture that enables a central authentication agency to govern attempts by a user to initiate a transaction. The kinds of transactions to which the invention is applicable include electronic access to communication systems, financial systems, computer networks, and interactive television and entertainment systems and physical access to secure locations. A fundamental principal of the invention is the central generation of an identifier that is unique to each transaction attempt. The identifier could, for example, be the time and date of the attempt, it could be a random number that is generated in the authentication agency each time a transaction is attempted or some other identifier number or code that is apparently not repeated or is not periodic within the time span of the transactions being attempted.

In the inventive architecture, authentication signals pass through two branches, a user branch and an authentication agency branch. The authentication signals passing through the two branches are then compared and a permit signal generated if the comparison is successful. The permit signal is then passed to the appropriate application device to allow the transaction to proceed. The application device may be, for example, a switch in a telecommunications system, a network access point into a computer or interactive television network, or a lock into a secured area.

The user attempting to initiate a transaction operates an access module which may, for example, be contained in a cellular telephone, a computer, an ATM access point, or within a lock securing a physical entry point. The access module must provide a means for user identification. For example, the user identification may be entered through an encoded card or key, or through a keyboard or keypad. For a cellular telephone, a user could insert a magnetically encoded card or other form of enabling key that contains a personal identification number (PIN). For an ATM or computer, a keyboard or key pad could be used to enter the user's personal identification information.

The architecture also includes transformation or encryption of the access information at various points in the two branches. The particular application is analyzed for its vulnerability to various forms of eavesdropping or interception by outsiders or various forms of interception by dishonest employees. This analysis will dictate the placement of various forms of transformation or encryption in the system. The transformations can be reversible or irreversible. The placement of the transformations or encryption steps can be either symmetric or asymmetric so long as the total transformation in the user branch is the same as the total transformation in the authentication agency branch by the time the signals are compared.

One important area of application of the invention is the field of telecommunications. In particular, the field of wireless communications such as cellular mobile radio. In this application, the following sequence of events could take place. The user enables the calling telephone by use of a telephone enabling key that contains the PIN identified with the user or with the telephone set itself. The user then lifts or otherwise activates the calling telephone handset to make the call. The calling telephone number is automatically sent to the central office which is the authentication agency. The central office generates a transaction identifier unique to that call attempt. The transaction identifier could be the date and time of the call attempt. The transaction identifier is then transmitted back to the user. An authentication code generator within the telephone combines the transaction identifier and the user's PIN to generate an authentication code. The authentication code is then transmitted back to the central office for comparison.

Within the central office, the telephone number of the calling telephone is routed to a database which looks up the associated user's PIN. The PIN and the transaction identifier are passed to an authentication code generator within the central office to generate an authentication code for comparison with the authentication code generated in the user's telephone. The comparison is made and, if successful, a permit signal is passed into the switching system to permit the call to proceed.

In a wireless communication system such as this, the transmission of the authentication code from the calling telephone to the central office is a point of particular vulnerability. In prior arts systems eavesdroppers, intercepting the authentication code, could build this code into their own telephone set and subsequently make unauthorized calls to be billed to the original user. However, in the system of the invention, since the authentication code is different for each call attempt, this is not possible. A more sophisticated unauthorized user may intercept both the transaction identifier and the authentication code and attempt to derive the PIN number. To protect against such an unauthorized user, the call identifier (e.g., calling telephone number) and PIN can be combined by means of an irreversible transform.

Analysis of the vulnerabilities of a particular system could suggest the use of additional transformations or encryption steps at different points in the system. For example, in the telephone set the PIN and calling telephone number could be combined in an initial transformation step which could be an irreversible transform. The irreversible transform of the calling telephone number and PIN or an encryption thereof would be stored within the central office's user identifier source (database) so that even within the central office the PIN is not available. The transform of the calling telephone number and PIN could be transmitted in the clear or encrypted between network elements. In this realization of the invention, the PIN is never stored or transmitted by any of the system's elements. As another security measure, the authentication codes could be encrypted or transformed with PIN (or an encrypted PIN), in both branches before the two signals are compared.

In all of the above variations, the comparison of two authentication signals will be successful if the successive application of the various transformations in the user branch produces the same total transformation as the successive application of the transformations on the central office side. However, irreversible transforms and all transforms or encryptions preceding them must be identical in both branches.

In all of these variations the authorized user has an advantage over the unauthorized user seeking to determine a usable PIN because the system architecture of the invention never requires application or derivation of an inverse transformation or the decryption of the signals. All signals are compared in a transformed or encrypted state. This places the unauthorized user in a very disadvantageous position and further protects the user's PIN number from being determined. All of the required transformation and encryption steps within the telephone set can be accomplished within a single microprocessor chip.

Another important application of the invention is in connection with access to automatic teller machines. In such machines the user inserts a magnetically encoded card and then manually enters a PIN number. This type of system is susceptible to interception of the PIN number as it is transmitted to the banking institution's central computer. Application of the invention would prevent an intercepted PIN number from being used subsequently to make unauthorized transactions, since the authorization code is different for each transaction. The use of an irreversible transform within the ATM access module would prevent a more sophisticated intruder from analyzing the transmitted signal to determine the user's PIN even if the intruder knew both the request identifier and the transform involved. Other financial transactions that could be similarly protected are money wire transfers and the presentation of personal credit cards.

In addition to controlling electronic access to various financial systems, the invented method and apparatus could be used to protect physical access to a secured location. In this case the permit signal, instead of controlling electrical access to a system, would control a physical lock.

FIG. 1 shows an exemplary device of the invention including an information generator 1 an authentication agency 2, and a transaction device 3. Within the information generator 1, a requesting means 4 transmits a transaction request to the authentication agency 2 together with information identifying the information generator. A first user identifier source 5 transmits the user identifier such as the user's PIN, to the first authentication code generator 6. The request is received by the request identifier generator 7 and the information identifying the information generator 1 is received by the second user identifier source 8. The request identifier generator 7 produces a request identifier unique to that particular transaction request and passes it to the first authentication code generator 6 and the second authentication code generator 9. The second user identifier source 8 obtains the user's PIN and passes it to the second authentication code generator 9. The first authentication code generator 6 and the second authentication code generator 9 produce first and second authentication codes and pass them to a comparator 10 for comparison.

A successful comparison of the two authentication codes will result in generation of a permit signal which is then passed to the transaction controller 11. The transaction controller 11 will then permit the information from the information source 12 to complete the transaction that is being attempted whether it be the electrical access to another system or physical access to a security area. For transactions involving independent information generation, the requesting means 16 and first authentication code generator 19 would form the nucleus of a transaction access module.

FIG. 2 shows an exemplary device of the invention in which the transaction involved is the transmission of information from an information generator 13 through a primary transmission path 15 to a communication terminal outside of the system. The transmission through the primary transmission path 15 is controlled by an authentication agency 14. The information generator includes a requesting means 16 which may have a key port 17. The requesting mean presents the transmission request to the authentication agency 14. The information generator 13 also includes a first user identifier source 18 which transmits the first user identifier to a first authentication code generator 19 through a first user identifier access port 20. In the authentication agency 14 the transmission request is presented to a request identifier generator 21 which generates a request identifier unique to that particular request. In a telecommunication system, the request identifier could be the time and date of the request, information which is readily available within a central office, or it could be a random number or pseudo random number generated by any one of the random number generators known in the art. The request identifier is transmitted by a second transmitter 29 to the first authentication code generator 19 through the first request identifier access port 23 and to a second authentication code generator 24 through a second request identifier access port 25.

In the authentication agency 14 the transmission request, which also contains information identifying the information generator 13, is transmitted to a second user identifier source 26 through a second transmission request access port 27. The second user identifier source 26 accesses its database to determine the user identifier corresponding to the information generator 13 and transmits it through a third transmitter 28 to the second authentication code generator 24 through the second user identifier access port 31.

The first authentication code generator 19 includes a first transformer for transforming the first user identifier and the first request identifier to produce a first authen-

tication code. The transformation produced by the transformer is advantageously an irreversible transform. However, some applications with lesser privacy requirements may use a reversible transform. The second authentication code generator 24 includes a second transformer for transforming the second request identifier together with the second user identifier to produce a second authentication code. The first authentication code is transmitted by means of a first transmitter 30 to a comparator 35 through a first authentication code access port 33. The second authentication code is transmitted by means of a fourth transmitter 32 to the comparator 35 through a second authentication code access port 34. The comparator includes a comparing means for comparing the first and second authentication codes. If the comparison is successful a permit signal is generated in the comparator 35 and transmitted by means of fifth transmitter 36 to a transmission controller 37 through a permit signal access port 38. The transmission controller 37 then permits the transmission of information from the information source 39 within the information generator 13 through the primary transmission path 15.

The first authentication code generator 19 may contain the first encryption means for encrypting the first user identifier. In this case the second user identifier source 26 must either store the user identifiers in encrypted form or must contain a second encryption means for encrypting the second user identifier when it is accessed. If the user identifiers are employed in encrypted form, then successive application of the first encryption means and the first transform must produce a total transformation which is identical to successive application of the second encryption means and the second transformer. This can be accomplished either by making the two encryptions identical and the two transformations identical or by making the encryptions and transformations different from one another such that the successive application of the two is identical in the two branches of the system.

Depending upon an analysis of the vulnerabilities of the particular system, the comparator 35 may include transformers at the first authentication code access port 33 and the second authentication code access port 34. These transformers may produce identical transformations or transformations that ultimately produce identical total transformations, as explained above.

FIG. 3 shows a device of the invention in which the vulnerability analysis has indicated the advisability of transmitting the request identifier as a transform. In this case the third transmitter 42 is also adapted for transmitting the second user identifier to the second transmitter 43 and the second transmitter 43 includes a third transformer for transforming the request identifier together with the second user identifier.

FIG. 4 shows an exemplary device of the invention in which the comparator 45 is associated with the transaction device 47. This would be the case for example, if a commercial entity went into the business of being an authentication agency and offered authentication services to different entities that controlled the transaction controller 44.

FIG. 5 illustrates the steps in the inventive process. Either simultaneously or in the following sequence; a transaction is requested 48, a first user identifier is introduced 49, and information is transmitted 50. The transaction request results in generation of a request identifier 51 and database access of a second user identifier 52. The request identifier and the first user identifier are used to generate the first authentication code 53 and the second user identifier and request identifier generate a second authentication code 54. The first authentication code and second authentication code are compared and if the comparison is successful the transaction is authorized 55. The authorization produces control of the transaction 56.

FIG. 6 illustrates another level of security in which the information generator 57 includes a third transformation/encryption means 58 for combining the first authentication code and the first user identifier. In addition, the authentication agency 59 includes a fourth transformation/encryption means 60 for combining the second authentication code and the second user identifier. The comparator 61 includes a fifth encryption means at the first authentication code access port 62 and a sixth encryption means at the second authentication code access port 63. Successive application of the first encryption means and the first transformer within the first authentication code generator 64, the third encryption means 58 and the fifth encryption means at the first authentication code access port 62 produces an identical transformation to the successive application of the second encryption means within the second user identifier source 65, the second transformer within the second authentication code generator 66, the fourth encryption means 60 and the sixth encryption means within the comparator at the second authentication code access port 63.

What is claimed:

1. In an information transmission system comprising an authentication agency, a primary transmission path, a switch in the primary transmission path, and an information generator with a station identifier, an authentication method comprising the steps of:

introducing a first user identifier from a first user identifier source into a first authentication code generator within the information generator;

transmitting a transmission request from the information generator to the authentication agency;

transmitting the station identifier from the information generator to the authentication agency; accessing a record in a second user identifier source of the user identifier corresponding to the station identifier in response to the transmission request;

forwarding the second user identifier from the second user identifier source to a second authentication code generator within the authentication agency;

generating a request identifier in a request identifier generator, in response to the transmission request;

transmitting the request identifier from the request identifier generator to the first and second authentication code generators;

generating a first authentication code in the first authentication code generator and a second authentication code in the second authentication code generator in response to the request identifier and the first and second user identifiers;

transmitting the first and second authentication codes to a comparator;

comparing the first and second authentication codes and generating a permit signal only if the comparison is successful, showing that the first user identifier and the request identifier have experienced the same total transformation as the second user identifier and the request identifier; and

transmitting the permit signal to the switch, enabling information flow through the primary transmission path, whereby information flow through the primary transmission path is permitted only after successful comparison of the first and second authentication codes.

2. A method of claim 1 in which the first authentication code and the second authentication code are generated through use of identical irreversible transforms.

3. A method of claim 2 including a step of encrypting the user identifier.

4. A method of claim 1 in which the first authentication code and the second authentication code are generated through use of encryption transforms.

5. A method of claim 1 in which the request identifier includes the time and date of the transmission request.

6. A method of claim 1 in which the request identifier is a number that is not repeated within the time span of the transmission request.

7. A method of claim i in which the first authentication code and the second authentication code are generated through use of identical transforms.

8. A method of claim i in which the first authentication code is generated through use of a first transform, comparison of the first authentication code includes use of a second transform, the second authentication code is generated through use of a third transform, and comparison of the second authentication code includes use of a fourth transform, the transforms being such that successive application of the first and second transform is identical to the successive application of the third and fourth transform.

9. A method of claim 8 in which the first transform and the third transform are irreversible transforms.

10. A method of claim i in which the information generator communicates with the authentication agency by means of radio transmission.

11. A method of claim i in which introducing the user identifier into the first authentication code generator includes the step of introducing an enabling key into the information generator.

12. A method of a claim 1 in which transmitting the request identifier includes transforming the request identifier together with the second user identifier.

13. An authenticating information transmission system comprising an information generator, an authentication agency and a primary transmission path, the information generator communicating with the authentication agency, said agency controlling the primary transmission path, wherein the information generator comprises:

requesting means for presenting a transmission request to the authentication agency;

a first authentication code generator comprising a first user identifier access port, a first request identifier access port, a first transformer for combining a first user identifier and a first request identifier transmitted to the respective access port to produce a first authentication code, and a first transmitter for transmitting the first authentication code to the authentication agency; and

an information source for introducing information into the primary transmission path,

wherein the authentication agency comprises:

a request identifier generator comprising a first transmission request access port and a second transmitter for transmitting the request identifier to the first authentication code generator and to a second authentication code generator;

a user identifier source comprising a second transmission request access port and a third transmitter for transmitting a second user identifier to the second authentication code generator;

the second authentication code generator comprising a second request identifier access port, a second user identifier access port, a second transformer for combining the second request identifier and the second user identifier, transmitted to the respective access port to produce a second authentication code, and a fourth transmitter for transmitting the second authentication code to a comparator; and

the comparator comprising a first authentication code access port, a second authentication code access port, a comparing means for comparing the first authentication code and the second authentication code, transmitted to the respective access port, and producing a permit signal only if the first authentication code and the second authentication code, when compared by the comparing means, are equal, indicating a matching condition between the first and second authentication codes, and a fifth transmitter for transmitting the permit signal to the primary transmission path; and

wherein the primary transmission path comprises a transmission controller with a permit signal access port for authorizing transmission when the permit signal is transmitted to the permit signal access port.

14. A device of claim 13 in which the requesting means includes a key port for accepting an enabling key with the first user identifier.

15. A device of claim 14 in which the first authentication code generator includes first encryption means for encrypting the first user identifier.

16. A device of claim 15 in which the user identifier source includes a second encryption means for encrypting the user identifier.

17. A device of claim 16 in which successive application of the first encryption means and the first transformer produces an identical transformation to successive application of the second encryption means and the second transformer.

18. A device of claim 16 in which the information generator further includes a third transformation/encryption means for combining the first authentication code and the first user identifier, the authentication agency further includes a fourth transformation/encryption means for combining the second authentication code and the second user identifier, the comparator includes a fifth encryption means at the first authentication code access port and a sixth encryption means at the second authentication code access port, wherein successive application of the first encryption means, the first transformer, the third transformation/encryption means and the fifth encryption means produces an identical transformation to the successive application of the second encryption means, the second transformer, the fourth transformation/encryption means and the sixth encryption means.

19. A device of claim 13 in which the first transformer and the second transformer produce the same irreversible transform.

20. A device of claim 13 in which the first transformer and the second transformer produce reversible encryption transforms.

21. A device of claim 13 in which the request identifier generator transmits a request identifier including the time and date of the transmission request.

22. A device of claim 13 in which the request identifier generator transmits a request identifier that is not repeated within the time span of the transmission request.

23. A device of claim 13 in which the third transmitter is also adapted for transmitting the second user identifier to the second transmitter and the second transmitter includes a third transformer for transforming the request identifier together with the second user identifier.

24. A transaction request authentication process comprising the steps of:

introducing a first user identifier into a first authentication code generator, within a user device;

transmitting a transaction request to an authentication agency;

in the authentication agency, generating a request identifier and a second user identifier in response to the transaction request;

transmitting the request identifier to the first authentication code generator and to a second authentication code generator, within the authentication agency;

transmitting the second user identifier to the second authentication code generator;

generating a first authentication code in response to the first user identifier and the request identifier and a second authentication code in response to the second user identifier and the request identifier;

transmitting the first authentication code and the second authentication code to a comparator, within the authentication agency;

generating a permit signal in the comparator in response to the first and second authentication codes; and

transmitting the permit signal to a transaction device, thereby authorizing a transaction to proceed.

25. A method of claim 24 including the step of encrypting the first user identifier and the second user identifier.

26. A method of claim 24 in which the first authentication code and the second authentication code are generated using an irreversible transform.

27. A method of claim 24 in which the request identifier includes the time and date of the transaction request.

28. A method of claim 24 in which the request identifier is a number that is not repeated within the time span of the transmission request.

29. A method of claim 24 in which the first and second authentication codes are generated using an encryption transform.

30. A method of claim 24 including the steps of encrypting the first and second authentication codes.

31. A method of claim 24 including transforming the request identifier together with the second user identifier.

32. A transaction request authentication process comprising the steps of:

introducing a first user identifier into a first authentication code generator, within a user device;

generating a request identifier in the user device;

transmitting a transaction request and the request identifier to an authentication agency;

in the authentication agency, generating a second user identifier in response to the transaction request;

transmitting the request identifier to the first authentication code generator and to a second authentication code generator, within the authentication agency;

transmitting the second user identifier to the second authentication code generator;

generating a first authentication code in response to the first user identifier and the request identifier and a second authentication code in response to the second user identifier and the request identifier;

transmitting the first authentication code and the second authentication code to a comparator, within the authentication agency;

generating a permit signal in the comparator in response to the first and second authentication codes; and

transmitting the permit signal to a transaction device, thereby authorizing a transaction to proceed.

33. A transaction request authentication process comprising the steps of:

in an authentication agency, generating a request identifier and a user identifier in response to a transaction request from a user;

transmitting the request identifier to the user and to an authentication code generator;

transmitting the user identifier to the authentication code generator;

generating a first authentication code in the authentication code generator in response to the request identifier and the user identifier;

transmitting the first authentication code to a comparator; receiving into the comparator a second authentication code produced by the user in response to the request identifier;

generating a permit signal in the comparator in response to the first authentication code and the second authentication code; and transmitting the permit signal to a transaction device, thereby authorizing a transaction to proceed.

34. An information generator for use in an authenticating information transmission system comprising:

requesting means for presenting a transmission request to an authentication agency;

a first authentication code generator comprising a first user identifier access port, a first request identifier access port, a first transformer for combining a first user identifier and a first request identifier transmitted to the respective access port to produce a first authentication code, and a first transmitter for transmitting the first authentication code to the authentication agency; and

an information source for introducing information into the primary transmission path.

35. A device of claim 34 in which the first transformer is adapted for producing an irreversible transform.

36. An authentication agency for use in an authenticating transaction system comprising:

A request identifier generator comprising a first transaction request access port and a second transmitter for transmitting the request identifier to the first authentication code generator and to a second authentication code generator;

a user identifier source comprising a second transaction request access port, a third transaction request

access port and a third transmitter for transmitting the second user identifier to the second authentication code generator;

the second authentication code generator comprising a second request identifier access port, a second user identifier access port, a second transformer for combining the second request identifier and the second user identifier, transmitted to the respective access port to produce a second authentication code, and a fourth transmitter for transmitting the second authentication code to a comparator; and

the comparator comprising a first authentication code access port, a second authentication code access port, a comparing means for comparing the first authentication code and the second authentication code, transmitted to the respective access port, and producing a permit signal in response to the first and second authentication codes, and a fifth transmitter for transmitting the permit signal to the primary transaction path for authorizing the transaction to proceed.

37. A transaction access module for use in a authenticating transaction system comprising: requesting means for presenting a transaction request to an authentication agency; and a first authentication code generator comprising a first user identifier access port, a first request identifier access port, a first transformer for combining a first user identifier and a first request identifier to produce a first authentication code, and a first transmitter for transmitting the first authentication code to the authentication agency.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 5,343,529

DATED : August 30, 1994

INVENTOR(S) : Milton Goldfine, Marvin Perlman, Robert A. Montgomery

It is certified that error appears in the above-indentified patent and that said Letters Patent is hereby corrected as shown below:

Col. 6, Line 37: After "requesting" delete "mean" and insert --means--.

Col. 9, Claim 7: After "claim" delete "i" and insert --1--.

Claim 8: After "claim" delete "i" and insert --1--.

Claim 10: After "claim" delete "i" and insert --1--.

Claim 11: After "claim" delete "i" and insert --1--.

Signed and Sealed this

Seventh Day of March, 1995

Attest:

BRUCE LEHMAN

Attesting Officer

Commissioner of Patents and Trademarks

US006000608A

United States Patent [19]

Dorf

[11] Patent Number: 6,000,608

[45] Date of Patent: Dec. 14, 1999

[54] MULTIFUNCTION CARD SYSTEM

[76] Inventor: Robert E. Dorf, 904 Bromley Way, Raleigh, N.C. 27615

[21] Appl. No.: 08/891,261

[22] Filed: Jul. 10, 1997

[51] Int. Cl.[6] G06K 5/00

[52] U.S. Cl. 235/380; 235/375

[58] Field of Search 235/380, 375, 235/381, 382, 492, 493; 902/1, 2, 8, 10, 12, 22, 24, 25, 26, 27

[56] References Cited

U.S. PATENT DOCUMENTS

4,491,725	1/1985	Pritchard	235/375
4,700,055	10/1987	Kashkashian, Jr.	235/379
4,731,818	3/1988	Clark, Jr. et al.	379/144
4,831,647	5/1989	D'Avello et al.	379/91
4,900,903	2/1990	Wright et al.	235/380
4,951,308	8/1990	Bishop et al.	379/91
4,963,722	10/1990	Takeuchi	235/382.5
4,990,904	2/1991	Wright et al.	235/381
5,101,098	3/1992	Naito	235/475
5,144,649	9/1992	Zicker et al.	379/59
5,146,067	9/1992	Sloan et al.	235/381
5,147,021	9/1992	Maruyama et al.	194/217
5,212,369	5/1993	Karlisch et al.	235/380
5,227,612	7/1993	Le Roux	235/379
5,243,174	9/1993	Veeneman et al.	235/381
5,264,689	11/1993	Maes et al.	235/492
5,310,997	5/1994	Roach et al.	235/375
5,352,876	10/1994	Watanabe et al.	235/381
5,409,092	4/1995	Itako et al.	194/210
5,440,108	8/1995	Tran et al.	235/381
5,450,938	9/1995	Rademacher	194/206
5,469,497	11/1995	Pierce et al.	379/115
5,491,326	2/1996	Marceau et al.	235/381
5,500,514	3/1996	Veeneman et al.	235/381
5,504,808	4/1996	Hamrick, Jr.	379/144
5,511,114	4/1996	Stimson et al.	379/114
5,513,117	4/1996	Small	364/479
5,524,073	6/1996	Stambler	380/24
5,530,232	6/1996	Taylor	235/380
5,542,081	7/1996	Geronimi	395/800
5,557,516	9/1996	Hogan	364/406
5,559,885	9/1996	Drexler et al.	380/23
5,563,934	10/1996	Eda	379/144
5,572,004	11/1996	Raimann	235/380
5,577,109	11/1996	Stimson et al.	379/112
5,578,808	11/1996	Taylor	235/380
5,621,787	4/1997	McKoy et al.	379/144
5,652,421	7/1997	Veeneman et al.	235/381
5,682,027	10/1997	Bertina et al.	235/380
5,815,561	9/1998	Nguyen et al.	379/115

Primary Examiner—Thien Minh Le
Assistant Examiner—Daniel Felten
Attorney, Agent, or Firm—Stroock & Stroock & Lavan LLP

[57] ABSTRACT

Disclosed is a multifunction card system which provides a multifunction card capable of serving as a prepaid phone card, a debit card, a loyalty card, and a medical information card. Each card has an identification number comprising a bank identification number which assists in establishing communications links. The card system can be accessed from any existing point-of-sale (POS) device. The POS device treats the card as a credit or debit card and routes transaction data to a processing hub using the banking system. The processing hub coordinates the various databases corresponding to the various functions of the card.

66 Claims, 2 Drawing Sheets

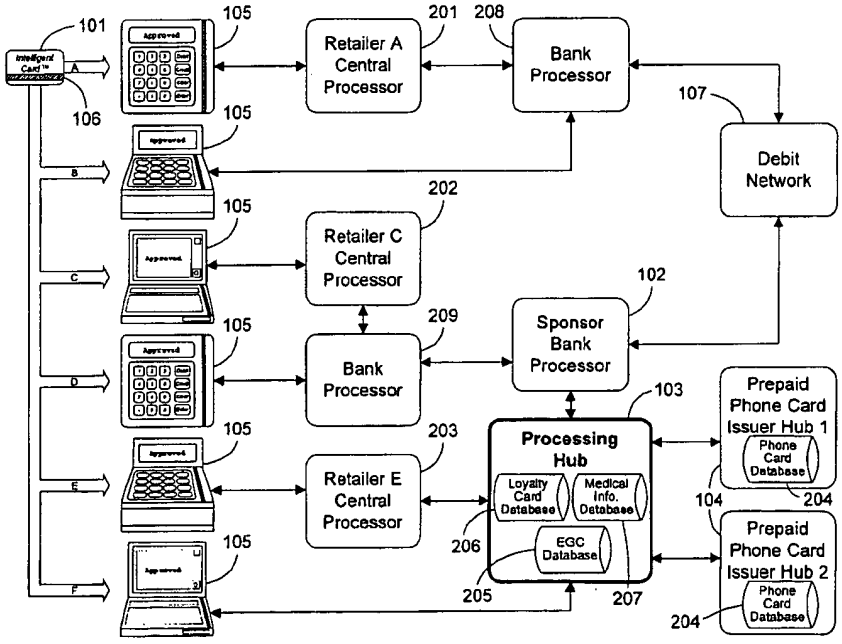


FIG. 1

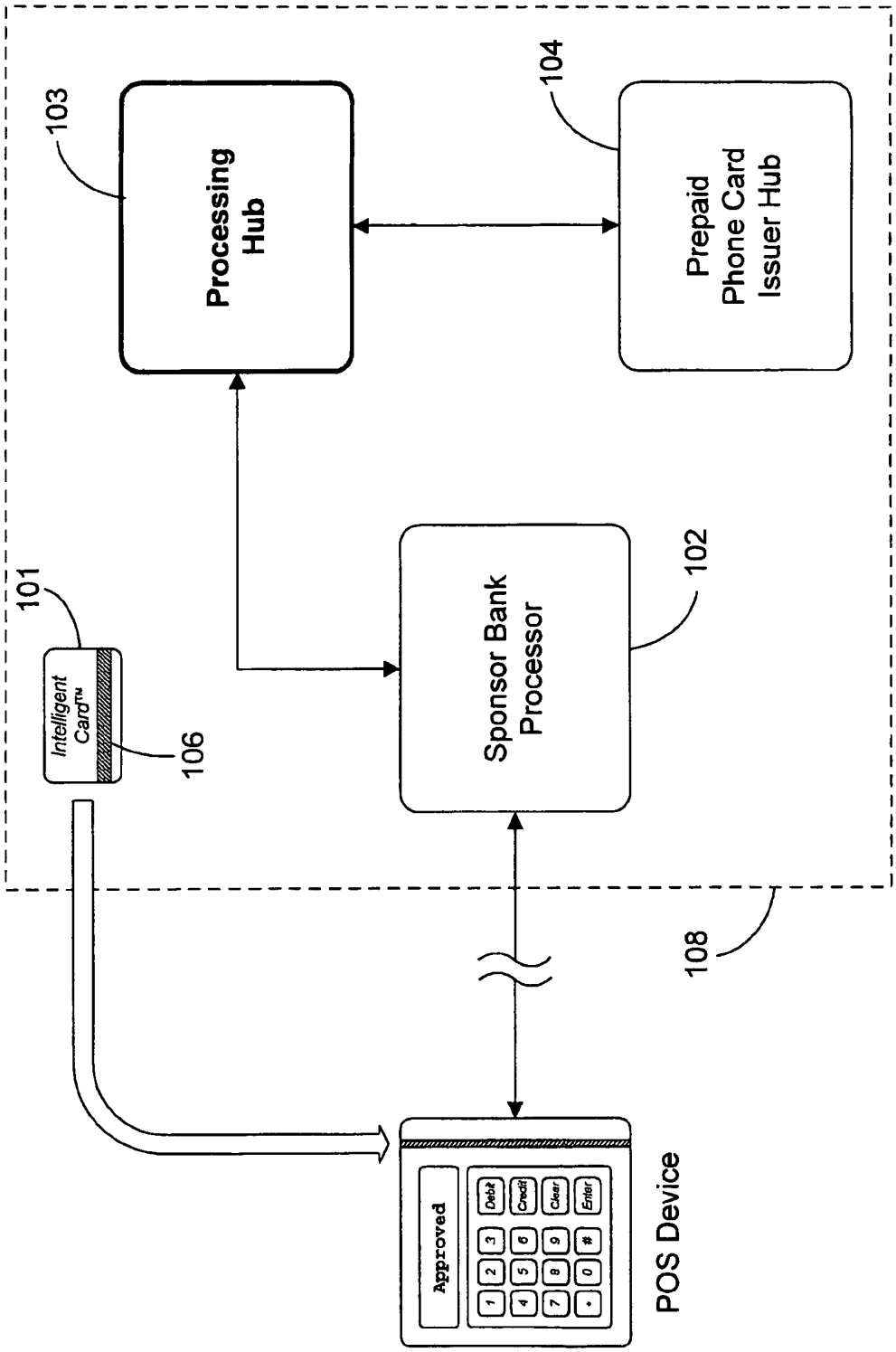
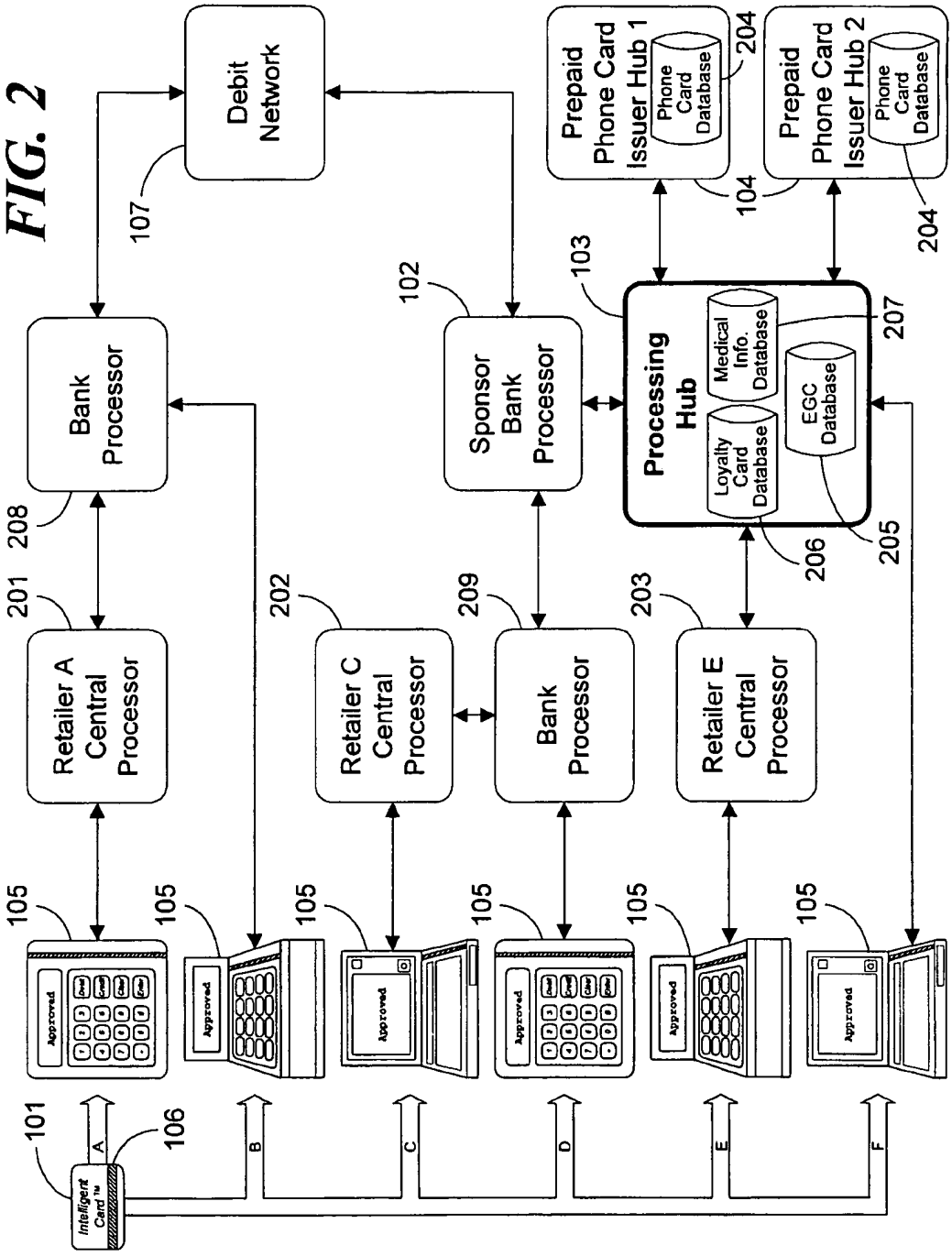

103
Processing Hub
104
Prepaid Phone Card Issuer Hub
101
Intelligent Card™
106
Sponsor Bank Processor
102
108
Approved
Debit
Credit
Clear
Enter
POS Device

FIG. 2


Debit Network
107
Prepaid Phone Card Issuer Hub 1
Phone Card Database
204
104
Prepaid Phone Card Issuer Hub 2
Phone Card Database
204
103
102
Bank Processor
Sponsor Bank Processor
Processing Hub
Medical Info. Database
207
Loyalty Card Database
EGC Database
206
205
208
201
202
209
203
Retailer A Central Processor
Retailer C Central Processor
Bank Processor
Retailer E Central Processor
105
Approved
101
Intelligent Card™
106
A
B
C
D
E
F

MULTIFUNCTION CARD SYSTEM

FIELD OF THE INVENTION

The present invention relates generally to debit card systems, both bank-issued and non-bank-issued, and more particularly to a multifunction card system that can be accessed by a variety of standard point-of-sale devices, by phone, by fax, or over the Internet.

BACKGROUND OF THE INVENTION

I. Debit Cards

Banking institutions often issue debit cards to their customers to give them access to funds from their savings or checking accounts. Such a debit card might be an on-line debit card or an off-line debit card. On-line debit cards, often referred to as automatic teller machine (ATM) cards, require a personal identification number (PIN) to be entered into an ATM or point-of-sale (POS) device in order to authorize the transaction. Once completed, the transaction clears the bank account immediately. Off-line debit cards function like credit cards, and usually carry the VISA® or MasterCard® logo. A retailer processes the card like a credit card and the customer signs a receipt. The funds then clear the bank account in one to three days.

While such debit cards are extremely useful and provide convenience for bank depositors, they generally do not serve a plurality of functions. Therefore, there is a need in the art for a debit/credit card capable of performing a plurality of functions, such as an electronic gift certificate card, a prepaid phone card, and a loyalty card, all in a real-time secure environment. There is also a need in the art for a system which can provide a card substitute for travelers checks and money orders which can be accepted by any POS device or ATM for financial transactions. Further, there is a need for a processing center which can manage such a multifunction card system.

II. Prepaid Phone Cards

Prepaid card systems are used by the telephone industry to allow customers to prepurchase long distance calling time. Such cards are typically purchased in predefined value increments. The card provides the customer with an amount of long distance calling time equivalent to the predefined value increment.

Each of the cards has an identification number printed or magnetically stored on it. The identification number is also stored in a record in a database maintained by the card issuer. This record also stores the predefined value of the card. When the cards are sent to the retail location from which they will be sold, the corresponding records in the database are activated, thus allowing the card to be used immediately by a customer. To use the card, the customer dials a toll free number to access the card issuer's system, enters the identification number, and then makes the desired long-distance call. During the call, the value of the card in the database is decremented accordingly. When the value of the card is exhausted, the call terminates. If the customer ends the call before the value of the card is exhausted, the remaining value may be used for additional calls. Once the entire value of the card has been used, it is discarded.

These prior art prepaid phone card systems have several disadvantages. First, since the cards are active while on the shelf in the retail location, they may be stolen by a thief and easily used. Second, the prior art systems do not allow the customer to purchase a card having any given value, nor do they allow the customer to recharge the value of the cards once the are depleted.

One way to address some of the drawbacks of prior art prepaid phone card systems would be to install activation terminals unique to the prepaid card issuer. This is referred to as a "closed system." U.S. Pat. No. 5,577,109 to Stimson et al. discloses such a closed system. In the Stimson system, the cards are not preactivated. Each of the retail locations from which cards are to be sold is provided with a dedicated activation terminal which allows the retail operator to set the value of the card at the time of the sale. The activation terminal connects to the card issuer's system to pass along the value amount and to request activation of the card. Depleted cards can be recharged in the same manner as they are sold. A serious disadvantage of the Stimson system is that it requires single-function dedicated hardware to be installed in each retail location, resulting in a very inflexible and expensive system.

Thus, there is a need in the art for a prepaid phone card activating system which is easily and inexpensively deployed, and which allows cards to be purchased in varying amounts and to be recharged without requiring the use of a closed system to handle the transactions.

III. Loyalty Cards

Loyalty cards are used to reward consumers for purchasing goods or services. For instance, airlines commonly reward frequent fliers with points for each mile flown with that airline. When the consumer accumulates a certain number of points, he or she is rewarded with free or discounted air fare. In this and other similar systems, the loyalty card issuer directly participates in the sale transaction. Such systems, however, do not allow a manufacturer of a product which is sold by an unrelated retailer to immediately reward the ultimate purchaser of the product with loyalty points. Since the manufacturer does not know of the ultimate sale until much later, if ever, it is difficult for such a manufacturer to conduct a loyalty program. Thus, there is presently no method for creating a product-specific loyalty card as opposed to a retailer-specific card. Nor is there a system for communicating loyalty data to databases not located at the retail establishment.

Furthermore, prior art loyalty programs generally do not credit the consumer's loyalty account in real-time as a purchase transaction takes place. Therefore, the consumer is unable to enjoy the benefits of their added loyalty points immediately. Finally, prior art loyalty programs commonly require significant startup efforts and expenses before the system is operational. Therefore, there is a need in the art for a real-time loyalty card system which is easily deployed, and which is capable of providing a product-specific loyalty card as well as a retailer-specific card. There is also a need for a system which can reward customers automatically for their loyalty and communicate this loyalty reward to databases other than at a retail location.

IV. Information Retrieval

Often, it is important to access certain types of information in a very fast and convenient manner. For example, a person's medical history can be extremely important in assessing the propriety of certain medical procedures during a medical emergency. Presently, in order to obtain a patient's medical history, the patient or his or her doctor must request the appropriate files from the patient's previous doctor(s). It often takes a number of days to receive the requested information. In a medical emergency, this delay is often far too long. Thus, there is a need for patients to have control over their own medical history data. Further, there is a need for this data to be instantly available to the patient, or the patient's doctor if the patient is incapacitated.

V. Multifunction Card

Due to the proliferation of various types of cards (e.g., credit/debit, long-distance calling, loyalty, etc.) over the last

couple of decades, it has become increasingly difficult to keep track of each individual card. There is a need for a card system which can serve a number of functions, thus allowing the consumer to have one card which may act as their card for financial transactions, long-distance telephone calls, loyalty information, and medical information.

SUMMARY OF THE INVENTION

The present invention solves the problems associated with prior art card systems by providing an improved multifunction card system. The multifunction card system comprises at least one electronic gift certificate card having a unique identification number encoded on it, the identification number comprising a bank identification number corresponding to the multifunction card system; means for receiving electronic gift certificate card activation data from an existing standard retail point-of-sale device when the electronic gift certificate card is swiped through the point-of-sale device, the electronic gift certificate card activation data comprising the unique identification number of the electronic gift certificate card and an electronic gift certificate activation amount; means for activating an account corresponding to the electronic gift certificate card with a value equal to the electronic gift certificate activation amount; and means for allowing a user of the electronic gift certificate card to purchase goods having a value up to the electronic gift certificate activation amount.

The multifunction card system further comprises at least one phone card having a unique identification number encoded on it, the identification number comprising a bank identification number corresponding to the multifunction card system; means for receiving phone card activation data from an existing standard retail point-of-sale device when the phone card is swiped through the point-of-sale device, the phone card activation data comprising the unique identification number of the phone card and a phone card activation amount; means for activating an account corresponding to the phone card with a value equal to the phone card activation amount; and means for allowing a user of the phone card to obtain long distance telephone calling time having a value up to the phone card activation amount.

In a preferred embodiment, the multifunction card system further comprises at least one loyalty card having a unique identification number encoded on it, the identification number comprising a bank identification number corresponding to the multifunction card system; means for receiving loyalty data from an existing standard retail point-of-sale device when the loyalty card is swiped through the point-of-sale device, the loyalty data comprising the unique identification number of the loyalty card and a purchase amount; and means for crediting an account corresponding to the loyalty card with a number of loyalty points proportional to the purchase amount.

Optionally, the multifunction card system of the present invention may also comprise at least one medical information card having a unique identification number associated with it, the medical information card belonging to a patient; a database comprising at least one record corresponding to the medical information card, the record containing medical history information about the patient; and means for allowing an authorized requester to obtain the medical history information about the patient using the unique identification number associated with the medical information card.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more fully understood by reference to the following detailed description when considered in conjunction with the following drawings wherein like reference numbers denote the same or similar portions or processes shown throughout the several Figures, in which:

FIG. **1** is a block diagram of the multifunction card system of the present invention; and

FIG. **2** is block diagram demonstrating the various ways in which a retail point-of-sale device might connect to the multifunction card system of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is a multifunction card system which allows for the activation of prepaid phone cards and the use of Electronic Gift Certificate™ cards, loyalty cards, debit cards, and medical information cards. Further, the system provides for the immediate linkage of these various functions. FIG. **1** illustrates the multifunction card system **108** of the present invention. The system **108** comprises a plurality of cards **101**, a sponsor bank processor **102**, and a processing hub **103**, which serves as the nerve center of the system **108**. If the system **108** is to provide prepaid phone cards, it will also include a prepaid phone card issuer hub **104** maintained by a prepaid phone card issuer. In order to achieve the desired functionality, the system **108** uses existing banking networks in a unique and novel way to gain access to virtually all existing retail point-of-sale (POS) devices **105**. These devices **105** include stand-alone POS terminals, cash registers with POS interfacing, computers with POS interfacing, and other similar devices which can be used to access the banking system. As used herein, POS device includes all such devices, whether data entry is effected by swiping a card through the device or by manual entry.

To access these POS devices, the operator of the system **108** must apply for and obtain a Bank Identification Number (BIN) from the American Banking Association. The BIN serves as a unique identifier of the multifunction card system **108** within the banking network. The BIN is encoded on a magnetic strip **106** on each card **101** in the system **108** as a part of the card's identification number. Alternatively or additionally, the BIN and identification number could be encoded as a bar code, embossed on the surface on the card **101** in numerals for manual entry, or provided by any other means known in the art.

Preferably, the BIN's first digit will be the same number as the first BIN digit used by a popular card issuer. This is because POS devices are preprogrammed to recognize only certain types of cards, such as those issued by VISA® and MasterCard®, American Express®, etc. As a rule, these POS devices must be reprogrammed before they will accept a new type of card. However, since POS devices already recognize cards issued by these popular card issuers, a new type of card will also be recognized by such devices if it has a BIN that begins with the same number used by one of the popular card issuers. Since VISA® and MasterCard® are the most universally accepted cards, the BIN of the multifunction card system **108** of the present invention preferably will begin with the same number used by either VISA® or MasterCard® (i.e., "4" or "5", respectively). By using one of these numbers, the card **101** will be recognized by almost all existing POS devices **105** as a debit or credit card, and its transactions will be automatically routed by the banking system to the correct destination. This occurs regardless of the type of POS device **105** used, since all such devices are designed to interface with the banking network. Although

the BIN number will preferably begin with a "4" or "5", it may begin with any number that is recognized by POS devices **105**.

The operator of the system **108** should also have a sponsoring bank whose bank processor **102** will serve as the link between the processing hub **103** and the banking network. Alternatively, the operator of the system **108** could itself be a banking institution.

By providing a means for any given POS device **105** to connect to the processing hub **103**, the system **108** allows a retailer to remotely activate or add value or loyalty data to a system card. The method by which this occurs is set forth more fully below in the context of the various functions of the card.

I. Prepaid Phone Card

A plurality of long distance service providers may contract with the operator of the multifunction card system **108** to issue prepaid phone cards **101** for use in the system **108**. Alternatively, a long distance service provider may itself be the operator of the system **108**. The long distance service provider will be referred to as a phone card issuer. A phone card issuer provides prepaid phone cards **101** to retailers who sell the cards **101** at their retail locations. Until activated, the cards **101** have no intrinsic value associated with them. Therefore, they may be placed on store shelves in easily accessible areas without the fear of losses due to theft. When a customer wishes to purchase or recharge one of the cards **101**, he or she informs the sales clerk of the monetary amount desired. Depending upon the system chosen by the particular phone card issuer, this amount may be one of a finite number of predefined amount increments, or may be selected by the customer. The clerk swipes the card **101** through the POS device **105**. Depending upon the amount of customization that has occurred at the retailer's location, there are a number of ways in which the POS device **105** may connect to the system's **108** processing hub **103** to carry out the transaction. FIG. **2** illustrates several of these methods.

The first two methods shown in FIG. **2**, methods A and B, are the most easily deployed, but cost the most on a per-transaction basis. To route information to the processing hub **103**, these methods employ the debit network **107** used by banking institutions. The retailer in method A (retailer A) has a central processor which controls each of its POS devices **105** and connects them to a processor **208** at a bank chosen by the retailer. Retailer B's POS device **105** connects directly to the bank processor **208**. Otherwise, the two methods are the same.

Banking regulations currently require that any transaction taking place over the debit network **107** must result in an actual transfer of funds. Since this phone card activation transaction is not a typical debit transaction, it is presently desirable to keep the official amount of the transaction to a minimum, yet still comply with the banking regulations. Therefore, regardless of the actual sale amount, the clerk enters a nominal transaction amount. In a preferred embodiment, the nominal transaction amount is keyed to the actual transaction amount (e.g., $0.01 nominal=$10.00 actual, $0.02 nominal=$20.00 actual, etc.). Therefore, the actual transaction amount can be ascertained from the nominal amount. In this embodiment, the card could only be activated or recharged in predefined increments. If the card is to have a fixed value, the activation amount could also be encoded on the magnetic strip **106** of the card **101** as part of the card's identification number.

In an alternate embodiment, the card could be activated or recharged in any amount desired by the customer. In this case, the nominal transaction amount would be a fixed value, such as $0.01. Once the nominal transaction amount is entered, the actual sale amount could then be entered on the PIN pad of the POS device **105** instead of the personal identification number (PIN) that would normally be entered when using a debit card. By entering the actual sale amount in this manner, it can be any desired amount.

In either case, before it transmits the data, the POS device **105** encrypts the information to be sent. This information includes the identification number read from the card's magnetic strip **106**, the nominal transaction amount, and the actual sale amount if it was entered into the PIN pad. The system **108** contains software which will decrypt and translate the data upon receipt. Once the encryption has taken place, the POS device **105** transmits the data either directly or via the central processor **201** to the bank processor **208**. The bank processor **208** receives the data and transmits it over the debit network **107**. The debit network **107** then forwards the data to the sponsoring bank's processor **102**. As mentioned earlier, the sponsoring bank is one which has agreed to operate as a link between the debit network **107** and the processing hub **103**.

As mentioned earlier, banking regulations as they currently exist require that transactions taking place over the debit network must result in a transfer of funds. Preferably, in order to comply with the banking regulations, the sponsoring bank transfers the nominal amount (e.g., $0.01) from one account belonging to the retailer to another account also belonging to the retailer. The bank processor **102** then forwards the data from the POS device **105** to the processing hub **103**.

In methods C and D, the retailers' central processor **202** or POS device **105**, respectively, again connect to a processor **209** at a retailer-chosen bank. By agreement between the operator of the multifunction card system **108** and the retailer-chosen bank, this bank processor **209** is programmed to recognize the multifunction card system's BIN and to forward the system's transactions directly to the sponsoring bank's processor **102** rather than using the debit network **107**. Since the debit network **107** is not used, it is not necessary to use a nominal sale amount, although such a method would nonetheless work and might be preferred by the retailer for security and bookkeeping purposes. The system **108** could instead be programmed to prompt the clerk for the appropriate information. As in methods A and B, the sponsor bank processor **102** forwards the necessary information to the processing hub **103**. Although methods C and D are more efficient than methods A and B on a per transaction basis, they require some customization at the retailer location to cause the retailer to connect to a bank processor **209** that recognizes the system's BIN.

Methods E and F are the least costly methods of connecting to the processing hub **103** (i.e., directly from the retailer's central processor **203** or from the POS device **105** itself). The connection may be made via a toll-free telephone line, a dedicated phone line, over the Internet, or any other standard communication means. Again, however, these methods require the most customization at the retailer location to cause the retailer's system to recognize the multifunction card system's cards and to route their transactions directly to the processing hub **103**. Such customization, however, still does not require reprogramming of the POS devices themselves. The connection method chosen may be adjusted to fit the individual retailer's needs.

Regardless of the method used, the data will eventually arrive at the processing hub **103**. If the transmission has taken place over the debit network **107**, the data must be

decrypted using equipment well known in the art for decrypting debit transaction data. Once the data is received and, if necessary, decrypted, the processing hub **103** recognizes the identification number of the card as being associated with a particular prepaid phone card issuer. Next, a security check is performed to verify that this transaction is originating from a retailer that is authorized to sell the prepaid phone cards. If the transaction is originating from an authorized retailer, the transaction will proceed. The processing hub **103** will then forward the card identification number, retail store and POS device information, and amount information to the issuer hub **104** maintained by the prepaid phone card issuer. The issuer hub **104** contains one or more phone card databases **204** which store information about each phone card. When the issuer hub **104** receives the data from the processing hub **103**, it activates the record in the phone card database **204** having the same identification number as the card **101**. The value field in the record is then increased by the appropriate purchased amount. If the card is of a fixed value, the record is simply activated. The issuer hub **104** then returns an authorization number which travels back along the same path to the originating POS device **105**. The customer may then dial the prepaid phone card issuer's toll free number, enter the card number and any required PIN, and obtain long distance calling time having a value up to the value of the card stored in the phone card database **204**.

Each activation or recharge transaction is recorded by the system **108**. At the end of the day, a report is preferably created for each card issuer and retail location so that their accounts can be reconciled. Transfer of funds between these parties may then take place by any commercially acceptable means.

II. Electronic Gift Certificate™ Card

The multifunction card system **108** of the present invention is also capable of providing an Electronic Gift Certificate™ (EGC) card **101** for a retail issuer. Such a card **101** could be sold by the retail issuer for making purchases only in the retail issuer's stores or for use in a plurality of stores. As in the phone card context, the customer would ask the sales clerk for an Electronic Gift Certificate™ card of the desired amount. If the customer already has an Electronic Gift Certificate™ card, he or she might ask the clerk to add the desired amount to the already existing balance. The clerk swipes the card **101** and enters the transaction amount, either directly or using a nominal amount and/or the PIN pad, depending upon whether the debit network **107** is to be used. Using one of the methods discussed above, the data then makes its way to the processing hub **103**.

Alternatively, the activation could occur by processing the card **101** as a typical debit card using the debit network **107**. In such a case, the retail issuer would maintain accounts with the sponsor bank. When an activation transaction takes place, the bank would transfer the activation amount from a general account to an account corresponding to the card. If the card is to be accepted at a number of retail locations, the account corresponding to the card could be opened in the name of the card holder if appropriate paperwork is submitted to the bank. In this manner, the card could be used at any retail location capable of processing debit transactions. This would allow the card to serve as a prepaid card substitute for travelers checks and money orders. Regardless of the way in which the card is processed, the transaction data eventually makes its way to the processing hub **103**.

Upon receipt of the transaction data, the hub **103** recognizes the card **101** as being an Electronic Gift Certificate™ card of the retail issuer and activates or recharges the card **101** in the appropriate amount in an EGC database **205** maintained at the processing hub **103**.

Optionally, the Electronic Gift Certificate™ card **101** could also be recharged using a credit card via an on-line connection to the processing hub **103**, such as over the Internet.

Once a card **101** has been activated or recharged, the recipient of the card **101** is allowed to make purchases using the card. If the card is only for use in the retail issuer's stores, the purchase transaction might proceed in much the same manner as the activation process. The clerk would swipe the card **101** and enter the purchase amount. If the transaction is to be transmitted over the debit network, a nominal transaction amount may be used, and the actual amount entered instead of the PIN. A special code is used to indicate that the transaction is a purchase transaction rather than an activation or recharge transaction. If the debit network is used, the code could be the first digit of the PIN, followed by the purchase amount, thus allowing the software of the system **108** to recognize the type of transaction and decrypt the data accordingly.

Upon receipt of the data via one of the methods described above, the processing hub **103** compares the purchase amount to the balance for the card in the EGC database **205**. If the balance is greater than the purchase amount, the processing hub **103** will decrement the record in the database and will send back an approval code which will allow the transaction to proceed. If a sufficient balance is not present, the processing hub **103** will notify the POS device **105** that the transaction may not proceed. Preferably, an automated toll free number is provided for the holder of the card **101** to verify the remaining balance. The processing hub **103** preferably maintains records of all transactions.

If the card **101** is for use in many retail locations, it would instead be processed during purchase transactions as a typical debit card, preferably using the debit network **107**. In this case, either the retail issuer or the cardholder must have an account with the sponsor bank. When a purchase transaction takes place, the clerk or cardholder simply swipes the card and receives back a response in the same manner as a normal debit transaction. If sufficient funds are present in the account corresponding to the card, the transaction will be approved. The sponsor bank then transfers the purchase amount from the retail issuer's or cardholder's account to an account belonging to the retail location at which the purchase occurred, which account may or may not be located at the sponsor bank. The transaction data is then forwarded to the processing hub **103** so that the EGC database **205** can be updated.

In a preferred embodiment, an Electronic Gift Certificate™ card could also be used to obtain long distance calling time in addition to making purchases in the retail issuer's store. The retail issuer could contract with a prepaid phone card issuer to provide the calling time. When the card **101** is activated, the phone card issuer simultaneously creates an entry in its phone card database **204** corresponding to the entry in the EGC database **205**. The card **101** can then be used in exactly the same manner as the prepaid phone card discussed above. In order to prevent the use of the Electronic Gift Certificate™ card simultaneously to make purchases and to obtain long distance calling time, a safety procedure is provided. When the card **101** is used to make a long distance call, the phone card issuer hub **104** instructs the processing hub **103** to seize the record corresponding to the card **101** in the EGC database **205**. With the record seized, the system **108** will not authorize any purchasing activity for the duration of the call. When the call terminates, the phone

card issuer hub **104** decrements the appropriate record in its phone card database **204** and instructs the processing hub **103** to do the same in the EGC database **205**. The record in the EGC database **205** is then unseized. When the card **101** is used to make a purchase, the processing hub **103** similarly instructs the phone card issuer hub **104** to seize the appropriate record in the phone card database **204** for the duration of the transaction. When the transaction is over, the records in the EGC database **205** and the phone card database **204** are decremented appropriately.

In the preferred embodiment of the invention, the retail issuer is also given the capability to award loyalty points to the bearer of the Electronic Gift Certificate™ card in recognition of purchases or recharges made. In such a case, the processing hub **103** maintains a separate loyalty card database **206**. When the Electronic Gift Certificate™ card bearer adds money to the card **101**, or makes a purchase using the card **101**, the system **108** may add a number of points proportional to the purchase price to the card's record in the loyalty card database **206**. Alternatively points could be awarded based upon the frequency of card usage rather than purchase amounts. In either case, when the card bearer reaches certain predefined point plateaus, he or she may be rewarded by the retail issuer with additional card value or with long-distance calling time.

III. Loyalty Card

Not unlike the loyalty feature add-on of the Electronic Gift Certificate™ card, the system **108** of the present invention may provide a separate loyalty card much like a frequent flier card that can have points added at virtually any POS device **105**.

A. Product/Manufacturer-Specific Loyalty Card

The card could be issued by a certain manufacturer to reward a customer with loyalty points for purchasing the manufacturer's product, regardless of the retail location of the purchase. This reward could be tied to the purchase of a single product type or to all of the manufacturer's products. The loyalty points awarded could be varied based upon any promotional campaigns being conducted by the manufacturer. Points are added to the card at participating retail locations which sell the manufacturer's product(s). The card **101** is swiped at any retail location, the purchase amount for the manufacturer's product is entered using the PIN pad of the POS device **105**, and the data is transmitted to the processing hub **103** using one of the methods described above. After receiving the data, the processing hub **103** credits the appropriate record in the loyalty card database **206** with a number of points proportional to the purchase price. The card is transportable to any participating retailer. The system **108** allows the manufacturer to connect to the processing hub **103** via an on-line connection to access the loyalty card database **206**. Again, the customer could be rewarded when certain point plateaus are reached.

B. Retailer-Specific Loyalty Card

Alternatively, the card could be issued by a particular retailer to reward customers for purchases made in the retailer's location(s). The retailer could award points for any purchase within the store, or could target special promotional items. The card would function in a manner similar to the product-specific card. Once again, the customer is rewarded when certain point plateaus are reached.

Alternatively, the loyalty data could be used to simultaneously credit other databases of the system **108**. For instance, instead of awarding loyalty points, the system could add value in real time to a record in the phone database **204** at the prepaid phone card issuer hub **104**, thus rewarding the customer with free phone time. Loyalty points might also be converted into a dollar value for use at the retail location. Optionally, the system **108** can keep records of a consumer's purchasing habits for marketing purposes. As with the manufacturer-specific card, the system **108** allows the retailer to connect to the processing hub **103** via an on-line connection to access the loyalty card database **206**.

IV. Information Retrieval Card

Finally, the multifunction card system **108** of the present invention is capable of providing an information retrieval card. In an exemplary embodiment, a medical information card which allows access and retrieval of a patient's complete medical history from a multitude of remote locations is provided. Each participating patient's medical information is stored in a record in a medical information database **207** maintained at the processing hub **103**. The record contains the identification number encoded on the patient's card **101**.

When medical history information data is needed, it may be requested by swiping the card **101** through a POS device **105** at a participating doctor's office or hospital. Preferably, a PIN is entered into the POS device **105** to ensure that only an authorized person is able to request the information. The POS device **105** would then send the request to the processing hub **103** via one of the routes described above. When the processing hub **103** receives the request from the authorized requester, it then immediately sends the information to the requestor via means preselected by the participating doctor's office or hospital. Such means may include electronic mail, facsimile, voice response, and other similar means. The medical history information may be updated by the patient or his or her doctor or insurer by forwarding new information to the operator of the system **108** via an on-line connection, over the Internet, by telephone, by facsimile, or by mail.

As a backup, the request could instead be made using a computer, wherein the computer connects to the processing hub **103** via the Internet or by direct modem connection. The requestor might be allowed to view, print, or download the appropriate medical history information. Alternatively, the request could be made by facsimile or by calling an automated toll free number and entering the card number.

In order to allow a cardholder to keep track of medical savings accounts or various other means for paying for medical services (e.g., Medicare), the system **108** also allows access to a database which maintains the medical funds for the cardholder. As described above under the Electronic Gift Certificate™ section, the system **108** is able to authorize, reject, and cause money to be transferred based upon the cardholder's available medical funds.

V. Intelligent Card™

In the preferred embodiment of the invention, the multifunction card system **108** is capable of providing a single card **101** which is capable of performing all of the foregoing functions. Preferably, the system **108** also allows for the card **101** to be used as an on-line debit card after the cardholder registers with the system. In order to let the system **108** know which function or functions the card **101** is serving in any particular transaction, a code is entered into the PIN pad of the POS device from which the transaction is originating. Alternatively, the system **108** could prompt the user to indicate the proper card function and the databases that must be accessed. Based upon this input, the system **108** carries out the appropriate actions. The system **108** can access each of the databases discussed above and can simultaneously increase or decrease each database as needed by the type of transaction occurring.

VI. Processing Hub Technical Details

The processing hub **103** of the present invention provides front-end POS device management and message processing

for card authorization and activations. The processing hub **103** can be implemented using any computer having acceptable processing and storage capacity. It preferably comprises a Stratus RADIO Cluster™, which is a scaleable system based upon the standard Intel Pentium processor. The Stratus RADIO Cluster™ provides the processing hub **103** with a high degree of reliability and fault-tolerance. Since the Stratus system is scaleable, an adequate degree of redundancy can be provided in order to reduce the impact of individual failures. In addition, as demand for the multifunction card system increases, the processing hub **103** can be scaled to meet increasing demands for processing power and storage availability. The modular design of such a hub is upgradable for long term capacity planning and expansion.

The software of the system is preferably written in the C, Force, and Foxpro programming languages. The C language programs are preferably written to interface with specialty external interface boards. Force is preferably used for all on-line transaction processing, while Foxpro preferably provides for database management and the user interface. Since Force and Foxpro share database file structures, on-line transactions may be viewed by the system operators using the Foxpro interface.

In order to provide further reliability, all applications and data are replicated and synchronized across the processing hub **103** by Isis Reliable software. Load distribution among the modules is automatically controlled by the software to improve the response time and throughput. External communications nodes provide the necessary interface requirements of physical connectivity, protocol, message transmission, message validation, and message processing.

While the multifunction card system herein described constitutes the preferred embodiment of the present invention, it is to be understood that the invention is not limited to this precise form of system, and that changes may be made therein without departing from the scope of the invention which is defined in the following claims.

I claim:

1. A multifunction card system, comprising:

a. at least one electronic gift certificate card having a unique identification number encoded on it, said identification number comprising a bank identification number approved by the American Banking Association for use in a banking network, said identification number corresponding to the multifunction card system;

b. means for receiving electronic gift certificate card activation data from an unmodified existing standard retail point-of-sale device when said electronic gift certificate card is swiped through the point-of-sale device, said electronic gift certificate card activation data comprising the unique identification number of the electronic gift certificate card and an electronic gift certificate activation amount;

c. means for activating an account corresponding to the electronic gift certificate card with a balance equal to the electronic gift certificate activation amount;

d. means for allowing a user of the electronic gift certificate card to purchase goods and services having a value up to the balance of the account corresponding to the electronic gift certificate card; and

e. means for decreasing the balance of the account corresponding to the electronic gift certificate card by the value of the goods and services purchased.

2. A multifunction card system as recited in claim **1**, further comprising:

a. means for receiving electronic gift certificate card recharge data from an existing standard retail point-of-sale device when said electronic gift certificate card is swiped through the point-of-sale device, said electronic gift certificate card recharge data comprising the unique identification number of the electronic gift certificate card and an electronic gift certificate recharge amount; and

b. means for increasing the balance of the account corresponding to the electronic gift certificate card by the electronic gift certificate recharge amount.

3. A multifunction card system as recited in claim **1**, wherein the first digit of said bank identification number is selected from the group consisting of four and five.

4. A multifunction card system as recited in claim **1**, further comprising means for allowing a user of the electronic gift certificate card to obtain long distance telephone calling time, wherein the total of the value of the goods and services purchased and the long distance telephone calling time obtained cannot exceed the balance of the account corresponding to the electronic gift certificate card.

5. A multifunction card system as recited in claim **4**, wherein said means for receiving electronic gift certificate activation data from an existing standard retail point-of-sale device when said electronic gift certificate card is swiped through the point-of-sale device employs the banking network.

6. A multifunction card system as recited in claim **4**, further comprising means for associating loyalty data with the electronic gift certificate card based upon usage of the electronic gift certificate card.

7. A multifunction card system as recited in claim **1**, further comprising means for associating loyalty data with the electronic gift certificate card based upon usage of the electronic gift certificate card.

8. A multifunction card system as recited in claim **1**, wherein said means for receiving electronic gift certificate activation data from an existing standard retail point-of-sale device when said electronic gift certificate card is swiped through the point-of-sale device employs the banking network.

9. A multifunction card system as recited in claim **1**, further comprising:

a. at least one phone card having a unique identification number encoded on it, said identification number comprising a bank identification number approved by the American Banking Association for use in a banking network, said identification number corresponding to the multifunction card system;

b. means for receiving phone card activation data from an unmodified existing standard retail point-of-sale device when said phone card is swiped through the point-of-sale device, said phone card activation data comprising the unique identification number of the phone card and a phone card activation amount;

c. means for activating an account corresponding to the phone card with a balance equal to the phone card activation amount;

d. means for allowing a user of the phone card to obtain long distance telephone calling time having a value up to the balance of the account corresponding to the phone card; and

e. means for decreasing the balance of the account corresponding to the phone card by the value of the long distance telephone calling time obtained.

10. A multifunction card system as recited in claim **9**, further comprising:

a. means for receiving phone card recharge data from an existing standard retail point-of-sale device when said phone card is swiped through the point-of-sale device, said phone card recharge data comprising the unique identification number of the phone card and a phone card recharge amount; and

b. means for increasing the balance of the account corresponding to the phone card by the phone card recharge amount.

11. A multifunction card system as recited in claim **9**, wherein a single card with a single identification number can function as an electronic gift certificate card and as a phone card.

12. A multifunction card system as recited in claim **1**, further comprising:

a. at least one loyalty card having a unique identification number encoded on it, said identification number comprising a bank identification number approved by the American Banking Association for use in a banking network, said identification number corresponding to the multifunction card system;

b. means for receiving loyalty data from an existing standard retail point-of-sale device when said loyalty card is swiped through the point-of-sale device, said loyalty data comprising the unique identification number of the loyalty card and purchase data; and

c. means for crediting an account corresponding to the loyalty card with loyalty points based upon the purchase data.

13. A multifunction card system as recited in claim **12**, wherein a single card with a single identification number can function as an electronic gift certificate card and as a loyalty card.

14. A multifunction card system as recited in claim **1**, further comprising:

a. at least one medical information card having a unique identification number associated with it, said medical information card belonging to a patient;

b. a database comprising at least one record corresponding to said medical information card, said record containing medical history information about the patient; and

c. means for allowing an authorized requester to obtain the medical history information about the patient using the unique identification number associated with the medical information card.

15. A multifunction card system as recited in claim **14**, wherein a single card with a single identification number can function as an electronic gift certificate card and as a medical information card.

16. A prepaid phone card system, comprising:

a. at least one phone card having a unique identification number encoded on it, said identification number comprising a bank identification number approved by the American Banking Association for use in a banking network, said identification number corresponding to the prepaid phone card system;

b. means for receiving phone card activation data from an unmodified existing standard retail point-of-sale device when said phone card is swiped through the point-of-sale device, said phone card activation data comprising the unique identification number of the phone card and a phone card activation amount;

c. means for activating an account corresponding to the phone card with a balance equal to the phone card activation amount;

d. means for allowing a user of the phone card to obtain long distance telephone calling time having a value up to the balance of the account corresponding to the phone card; and

e. means for decreasing the balance of the account corresponding to the phone card by the value of the long distance telephone calling time obtained.

17. A prepaid card system as recited in claim **16**, further comprising:

a. means for receiving phone card recharge data from an existing standard retail point-of-sale device when said phone card is swiped through the point-of-sale device, said phone card recharge data comprising the unique identification number of the phone card and a phone card recharge amount; and

b. means for increasing the balance of the account corresponding to the phone card by the phone card recharge amount.

18. A prepaid phone card system as recited in claim **16**, wherein the first digit of said bank identification number is selected from group of numbers consisting of the numbers four and five.

19. A prepaid card system as recited in claim **16**, wherein said means for receiving phone card activation data from an existing standard retail point-of-sale device when said phone card is swiped through the point-of-sale device employs the banking network.

20. A loyalty card system, comprising:

a. at least one loyalty card having a unique identification number encoded on it, said identification number comprising a bank identification number approved by the American Banking Association for use in a banking network, said identification number corresponding to the loyalty card system;

b. means for receiving loyalty data from an unmodified existing standard retail point-of-sale device when said loyalty card is swiped through the point-of-sale device, said loyalty data comprising the unique identification number of the card and purchase data; and

c. means for crediting an account corresponding to the loyalty card with loyalty points based upon the purchase data.

21. A loyalty card system as recited in claim **20**, wherein the first digit of said bank identification number is selected from a group of numbers consisting of the numbers four and five.

22. A loyalty card system as recited in claim **20**, wherein said means for receiving loyalty data from an existing standard retail point-of-sale device when said loyalty card is swiped through the point-of-sale device employs the banking network.

23. A method of activating or recharging a prepaid card having a unique identification number encoded on it, the identification number comprising a bank identification number approved by the American Banking Association for use in a banking network, said identification number corresponding to a prepaid card system, comprising the steps of:

a. swiping the card through an unmodified existing standard retail point-of-sale device;

b. entering an amount into the point-of-sale device;

c. transmitting the identification number and the amount from the point-of-sale device to a processing hub;

d. crediting an account balance in a database with the amount;

e. allowing a user of the card to purchase goods and services using the card; and

f. allowing a user of the card to obtain long distance telephone calling time using the card;

g. wherein the total of the value of the goods and services purchased and the long distance telephone calling time obtained using the card cannot exceed the account balance.

24. A method according to claim **23**, further comprising the step of associating loyalty data with the card based upon usage of the card.

25. A method according to claim **24**, further comprising the step of transferring loyalty data to a phone card issuer.

26. A method according to claim **23**, wherein said step of transmitting the identification number and the amount from the point-of-sale device to a processing hub is carried out at least in part via the banking network.

27. A method of activating or recharging a prepaid phone card having a unique identification number encoded on it, the identification number comprising a bank identification number approved by the American Banking Association for use in a banking network, said identification number corresponding to a prepaid phone card system, comprising the steps of:

a. swiping the phone card through an unmodified existing standard retail point-of-sale device;

b. entering an amount into the point-of-sale device;

c. transmitting the identification number and the amount from the point-of-sale device to a processing hub;

d. transmitting the identification number and the amount from the processing hub to a prepaid phone card issuer hub;

e. crediting an account balance in a phone card database with the amount; and

f. allowing a user of the phone card to obtain long distance telephone calling time having a value up to the account balance.

28. A method according to claim **27**, wherein said step of transmitting the identification number and the amount from the point-of-sale device to a processing hub is carried out at least in part via the banking network.

29. A method of adding points to a loyalty card having a unique identification number encoded on it, the identification number comprising a bank identification number approved by the American Banking Association for use in a banking network, said identification number corresponding to a loyalty card system, comprising the steps of:

a. swiping the loyalty card through an unmodified existing standard retail point-of-sale device;

b. entering purchase data into the point-of-sale device;

c. transmitting the identification number and the purchase data from the point-of sale device to a processing hub; and

d. crediting an account in a database with loyalty points based upon the purchase data.

30. A method according to claim **29**, wherein said step of transmitting the identification number and the purchase amount from the point-of-sale device to a processing hub is carried out at least in part via the banking network.

31. A method according to claim **29**, further comprising the step of allowing the owner of the loyalty card to redeem loyalty points for an item selected from the group consisting of goods, services, discounts on goods and services, long distance telephone calling time value, and money value.

32. A multifunction card system comprising:

a. at least one debit/medical services card having a unique identification number encoded on it comprising a bank identification number approved by the American Banking Association for use in a banking network;

b. a transaction processor receiving card data from an unmodified existing standard point-of-sale device, said card data including a unique identification number;

c. a processing hub receiving directly or indirectly said card data from said transaction processor; and

d. said processing hub accessing a first database when the card functions as a debit card and said processing hub accessing a second database when the card functions as a medical card.

33. The multifunction card system of claim **32**, wherein the unique identification number further comprises a medical identification number.

34. A system comprising:

a. at least one electronic gift certificate card having an electronic gift certificate card unique identification number encoded on it, said electronic gift certificate card unique identification number comprising a bank identification number approved by the American Banking Association for use in a banking network;

b. a transaction processor receiving electronic gift card activation data from an unmodified existing standard retail point-of-sale device, said electronic gift certificate card activation data including said unique identification number and an electronic gift certificate card activation amount;

c. a processing hub receiving directly or indirectly said activation data from said transaction processor; and

d. said processing hub activating an account corresponding to the electronic gift certificate card unique identification number with a balance corresponding to the electronic gift certificate activation amount.

35. The system of claim **34**, wherein the electronic gift certificate card activation amount is encoded in the unique identification number.

36. The system of claim **34**, wherein the electronic gift certificate card activation amount is entered at the point-of-sale device.

37. The system of claim **34**, wherein said processing hub allows a user of the electronic gift certificate card to purchase a value up to the balance corresponding to the electronic gift certificate activation amount.

38. The system of claim **34**, wherein:

a. said transaction processor receives electronic gift certificate card recharge data from the existing standard retail point-of-sale device, said electronic gift certificate card recharge data including said unique identification number and an electronic gift certificate card recharge amount; and

b. said processing hub increasing said amount corresponding to the electronic gift certificate card unique identification number with a balance corresponding to the electronic gift certificate card recharge amount.

39. The system of claim **34**, wherein the first digit of the bank identification number is selected from a group of numbers consisting of the numbers four and five.

40. The system of claim **34**, wherein the processing hub allows the use of the electronic gift certificate card to obtain phone calling time.

41. The system of claim **34**, further comprising:

a. a prepaid phone card issuer hub receiving directly or indirectly the electronic gift card activation data from said processing hub; and

b. said prepaid phone card issuer hub activating a record in a phone card database corresponding to the electronic gift certificate card unique identification number.

42. The system of claim 41, wherein the prepaid phone card issuer hub instructs the processing hub to seize the account corresponding to the electronic gift certificate card unique identification number where an electronic gift certificate card is used to make a call.

43. The system of claim 41, wherein the processing hub instructs the phone card issuer hub to seize the record corresponding to the electronic gift certificate card unique identification number when the electronic gift certificate card is used to make a transaction.

44. The system of claim 34, wherein the transaction processor is coupled to the banking network.

45. The system of claim 34, wherein the processing hub associates loyalty data with the electronic gift certificate card based upon the usage of the electronic gift certificate card.

46. The system of claim 34, wherein the activation data received at the processing hub is encrypted.

47. The system of claim 34, wherein the processing hub includes a loyalty card database.

48. The system of claim 34, wherein the processing hub includes a medical information card database.

49. The system of claim 34, wherein the processing hub includes an electronic gift certificate card database, a loyalty card database, and a medical information database.

50. A multifunction card system comprising:

a. at least one electronic gift certificate card having an electronic gift certificate card unique identification number encoded on it, said electronic gift certificate card unique identification number comprising a bank identification number approved by the American Banking Association for use in a banking network;

b. a transaction processor receiving electronic gift card activation data from an unmodified existing standard retail point-of-sale device, said electronic gift certificate card activation data including the electronic gift certificate card unique identification number and an electronic gift certificate card activation amount;

c. a processing hub receiving directly or indirectly said activation data from said transaction processor; and

d. said processing hub activating an account corresponding to the electronic gift certificate card unique identification number with a balance corresponding to the electronic gift certificate activation amount.

51. The multifunction card system of claim 50, wherein the electronic gift certificate card activation amount is encoded in the unique identification number.

52. The multifunction card system of claim 50, wherein the electronic gift certificate card activation amount is entered at the point-of-sale device.

53. The multifunction card system of claim 50, further comprising:

a. at least one phone card having a phone card unique identification number encoded on it, said phone card unique identification number comprising a bank identification number approved by the American Banking Association for use in a banking network;

b. said transaction processor receiving phone card activation data from said existing standard retail point-of-sale device, said phone card activation data including said phone card unique identification number and a phone card activation amount;

c. said processing hub receiving directly or indirectly said phone card activation data from said transaction processor and recognizing the phone card unique identification number of the phone card as being associated with a particular prepaid phone card issuer; and

d. said processing hub forwarding the phone card activation data to a particular prepaid phone card issuer hub.

54. The multifunction system of claim 53, wherein the particular prepaid phone card issuer hub contains at least one phone card database which stores information about each said phone card and activates the stored information to permit debiting of a predetermined value of phone calling in response to the activation data.

55. The multifunction system of claim 50, further comprising:

a. at least one loyalty card having a loyalty card unique identification number encoded on it, said loyalty card identification number comprising a bank identification number approved by the American Banking Association for use in a banking network;

b. said transaction processor receiving loyalty card activation data from said existing standard retail point-of-sale device, said loyalty card activation data including said loyalty card unique identification number and purchase data;

c. said processing hub receiving directly or indirectly said phone card activation data from said transaction processor; and

d. said processing hub crediting an account corresponding to the loyalty card with loyalty points based upon the purchase data.

56. The multifunction system of claim 50, further comprising:

a. at least one medical information card having a medical card unique identification number associated with it, said medical information belonging to a patient; and

b. said processing hub including at least one record corresponding to said medical information card, said record containing medical history information about the patient.

57. A multifunction card system comprising:

a. at least one card having a unique identification number encoded on it, said identification number comprising a bank identification number approved by the American Banking Association for use in a banking network;

b. a transaction processor receiving card activation data from an unmodified existing standard retail point-of-sale device, said card activation data including said unique identification number;

c. a processing hub receiving directly or indirectly said activation data from said transaction processor; and

d. said processing hub activating an account corresponding to the unique identification number, thereby permitting later access to said account.

58. The multifunction card system of claim 57, wherein said card is selected from the group consisting of an electronic gift certificate card, a phone card, a loyalty card, and a medical information card.

59. The multifunction card system of claim 57, wherein said card performs the functions of an electronic gift certificate card, a phone card, a loyalty card, and a medical information card.

60. A method of activating a prepaid card having a unique identification number encoded on it, the identification number comprising a bank identification number approved by the American Banking Association for use in a banking network, the method comprising the steps of:

a. swiping the card through an unmodified existing standard point-of-sale device;

b. transmitting the identification number and an activation amount from the point-of-sale device to a processing hub; and

c. activating an account in the processing hub corresponding to the identification number.

61. The method of claim **60**, further comprising:

a. transmitting the identification number and a recharge amount from the point-of-sale device to a processing hub; and

b. recharging the account in the processing hub corresponding to the identification number.

62. The method of claim **60**, further comprising entering the activation amount into the point-of-sale device.

63. The method of claim **60**, wherein the step of transmitting the identification number and the activation amount from the point-of-sale device is carried out at least in part over the banking network.

64. The method of claim **60**, further comprising allowing a user of the card to obtain calling time using the card.

65. The method of claim **60**, further comprising allowing a user of the card to purchase goods and services using the card.

66. The method of claim **60**, further comprising associating loyalty data with the card based upon usage of the card.

* * * * *